SPECIAL REPORT

ONC RELEASES FINAL RULE IMPLEMENTING CURES ACT INFORMATION BLOCKING PROHIBITION

March 18, 2020

McDermott Will & Emery

McDermott Will & Emery

SPECIAL REPORT

TABLE OF CONTENTS

LEARN MORE

For more information, please contact your regular McDermott lawyer, or:

JAMES A. CANNATTI III
PARTNER

jcannatti@mwe.com
Tel +1 202 756 8866

DANIEL F. GOTTLIEB
PARTNER

dgottlieb@mwe.com
Tel +1 312 984 6471

KAREN S. SEALANDER
PARTNER

ksealander@mwe.com
Tel +1 202 756 8024

SCOTT A. WEINSTEIN
PARTNER

sweinstein@mwe.com
Tel +1 202 756 8671

LI WANG
ASSOCIATE

lwang@mwe.com
Tel +1 310 551 9347

For more information about McDermott Will & Emery visit mwe.com

OVERVIEW

The Office of the National Coordinator for Health Information Technology (ONC) published its highly anticipated final rule to implement the "information blocking" prohibition of the 21st Century Cures Act by identifying conduct that is not information blocking. ONC's final rule more closely aligns the information blocking provisions with the HIPAA Privacy Rule's right of patient access, while maintaining robust limitations on practices by certified health IT developers, health care providers and other regulated actors that are likely to impede the flow of electronic health information. In this *Special Alert*, we analyze the final rule and suggest practical next steps for regulated actors and their vendors.

IN DEPTH

On March 9, 2020, the US Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) released its long-awaited final rule identifying conduct that does not constitute information blocking under Section 4004 of the 21st Century Cures Act. The final rule requires certain certified health IT developers, health care providers, health information networks (HINs) and health information exchanges (HIEs) (*i.e.*, actors) to comply with the information blocking provisions beginning six months after publication of the final rule in the *Federal Register* (compliance date). The information blocking provisions of the final rule align more closely with the HIPAA Privacy Rule than ONC's proposed rule. The final rule imposes robust limitations on practices that are likely to interfere with access, exchange or use of electronic health information (EHI). For more information on ONC's proposed rule, see our prior *On The Subject*.

In addition to finalizing the Cures Act's information blocking provision, the final rule finalizes changes to ONC's 2015 Edition Health IT Certification Criteria, Health IT Certification Program and other ONC authorities. On the same day that ONC released the final rule, the Centers for Medicare & Medicaid Services (CMS) released a companion final rule on related interoperability issues. For more information about the CMS final rule, see our separate *On the Subject*.

Political Context and Stakeholder Reactions

Together, the ONC and CMS final rules seek to achieve health care policy priorities for the Trump Administration, including advancing seamless health data exchange and placing patients firmly in control of their EHI. According to HHS, "these rules deliver on the Administration's promise to put patients at the center of their care by promoting patient access and use of their own health information and spurring the use of and development of new smartphone applications." National Coordinator for Health Information Technology Don Rucker predicted the final rule will "drive a growing patient-facing health care IT economy" that will enable patients to "manage their health care the same way they manage their finances, travel and every other component of their lives . . . [allowing them] to use the tools they want to . . . coordinate their own care on their smartphones."

As noted, Congress prohibited practices that block the access, exchange or use of EHI in the Cures Act in 2016. The final rule implements those provisions by defining eight categories of "reasonable and necessary" activities that do not constitute information blocking. The Cures Act information blocking provisions and ONC's information blocking proposals in the proposed rule sparked heated controversy and intense efforts to shape the final rule. As of this writing, industry reactions have been mixed, although relatively measured. The most vocal statements in opposition to the rule criticize the patient privacy risks posed by greater access to EHI by third-party mobile application developers and other persons who are not patients, their legal representatives or their health care providers.

This *Special Report* addresses:

- Key definitions in the information blocking provisions of the final rule;
- Discussion of what conduct is information blocking absent an Exception;
- Analysis of the information blocking Exceptions that describe permissible conduct under the final rule;
- Complaint process and enforcement; and

- Practical impact and next steps for health care industry stakeholders.

KEY DEFINITIONS

Who Is an Actor Subject to the Information Blocking Prohibition?

The final rule's information blocking prohibition regulates actors, which includes health care providers, certified health IT developers, and HINs and HIEs:

- *Health care provider*. Consistent with the proposed rule, the final rule adopts the definition of health care provider under the Public Health Services Act (PHSA) rather than the HIPAA regulations' more expansive definition of the term. The PHSA definition includes, for example, a hospital, skilled nursing facility, long-term care facility, renal dialysis facility, ambulatory surgical center, federally qualified health center, laboratory, group practice, physician, and certain other categories of health care facilities and clinicians as determined by HHS.
- *Certified health IT developer*. The final rule defines certified health IT developer as an individual or entity, other than a health care provider that self-develops health IT for its own use, that develops or offers health IT and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more health IT modules certified under ONC's Health IT Certification Program.
- *HIN or HIE*. ONC notably combines and narrows the proposed definitions for HINs and HIEs to eliminate confusion from commenters about distinguishing between the two terms. ONC finalizes a single, functional definition for HINs and HIEs, and limits the definition to only include networks or exchanges that are related to treatment, payment and health care operations as defined by the HIPAA Privacy Rule.

ONC also clarifies that in order to meet the definition of an HIN or HIE, the entity must enable the exchange of EHI among more than two unaffiliated parties (beyond the HIN or HIE itself). This change is intended to ensure that parties that act as intermediaries in essentially bilateral exchanges—for example, an intermediary that receives EHI from one party in a non-standardized format and converts it to standardized data for the receiving party—would not be an HIN or HIE for information blocking purposes. Thus, several entities that might have fit under the proposed rule's broad definitions of HIN and HIE are spared that fate—and the accompanying risk of $1 million plus civil monetary penalty exposure.

What Information Is Protected?

The information blocking prohibition applies to EHI, which ONC defines as electronic protected health information under the HIPAA regulations (EPHI) to the extent that the EPHI is part of a patient's electronic medical record or another designated record set under HIPAA, regardless of whether the records are used or maintained by or for a HIPAA covered entity. A designated record set includes:

- The medical records and billing records about individuals;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

- Records that are used, in whole or in part, by or for the covered entity to make decisions about individuals.

The EHI definition explicitly excludes psychotherapy notes maintained by a health care professional and information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

While the final rule aligns the definition of EHI with the HIPAA Privacy Rule's concept of EPHI contained in a designated record set, ONC's final definition of information blocking provides that until the date 24 months after the publication of the final rule in the *Federal Register*, EHI is limited to the data elements represented in the US Core Data for Interoperability (USCDI) standard adopted under the health IT certification provisions of the final rule. Consequently, the EHI covered by the information blocking prohibition for the 18-month period following the compliance date is only a subset of the EHI that will be subject to the information blocking prohibition after that date.

Notably, ONC removes electronic, consumer-generated health information that is not EPHI from the definition of EHI. In addition, the final rule does not expressly include health care providers' price information or payers' payment rates within the definition of EHI. However, such price and payment information would be EHI to the extent that it is included in claims for payment or other billing records maintained by a health care provider.

As under the proposed rule, data that has been de-identified in accordance with the HIPAA Privacy Rule's de-identification standard does not meet the final rule's definition of EHI.

WHAT IS INFORMATION BLOCKING?

Under the final rule, information blocking means a practice that:

- Except as required by law or covered by an Exception set forth in the final rule, is likely to interfere with access, exchange or use of EHI; and
- If conducted by a health IT developer, HIN or HIE, such developer, network or exchange knows, or should know, is likely to interfere with, prevent or materially discourage access, exchange or use of EHI; or
- If conducted by a health care provider, such provider knows is unreasonable and is likely to interfere with, prevent or materially discourage access, exchange or use of EHI.

In the preamble to the final rule, ONC reiterates the five categories of practices that it previously identified in the proposed rule as likely to interfere with access, exchange or use of EHI and that therefore could constitute prohibited information blocking. While ONC declines commenters' calls to revise or clarify the majority of examples of such practices that it provided in the proposed rule, ONC offers a few clarifications and some new examples.

The five categories of practices are as follows:

- *Restrictions on Access, Exchange or Use.* ONC clarifies that contract terms, beyond terms related to unreasonable fees or licensing terms, could result in a restriction on access, exchange and use of EHI. For example, ONC warns against an actor using a HIPAA Business Associate Agreement (BAA) to limit in a discriminatory manner disclosures that HIPAA's Privacy Rule would otherwise allow. ONC notes, as an example, that a

BAA should not permit access to EHI by certain health care providers for treatment purposes, while limiting access for the same purposes by a patient's other health care providers.

- *Limiting or Restricting the Interoperability of Health IT.* As a new example of a limitation or restriction of interoperability that may constitute prohibited information blocking, ONC notes, in the context of patients attempting to access their EHI via an actor's application programming interface (API), that an actor may not take steps to restrict the public availability of an endpoint necessary to access the actor's API.
- *Impeding Innovation and Advancements in Access, Exchange or Use of Health IT-Enabled Care Delivery.* While a refusal to license an interoperability element could raise information blocking concerns, ONC clarifies that an actor may refuse to license its interoperability element when the requestor is not seeking to use the interoperability element to connect with the actor or its customer to access, exchange or use EHI.

  ONC spends a considerable portion of the final rule preamble discussing the distinction between interference and education regarding patient-facing third-party applications. Attempting to address commenter concerns, ONC clarifies that actors may provide additional information to individuals about their chosen applications to receive EHI (*e.g.*, explaining advantages and disadvantages of accessing EHI through a third-party application, and associated risks). Such practices are unlikely to constitute information blocking if they meet the following criteria:

  - The information focuses on any current privacy and/or security risks posed by the technology or the third-party developer;
  - The information is factually accurate, unbiased, objective and not unfair or deceptive; and
  - The information is provided in a non-discriminatory manner.
- *Rent-Seeking and Other Opportunistic Pricing Practices.* ONC states that opportunistic pricing practices may constitute prohibited information blocking when they artificially increase costs for accessing, exchanging and using EHI, such as when an actor implements discriminatory pricing policies that have the obvious purpose and effect of excluding competitors from the use of interoperability elements.
- *Non-Standard Implementation Practices.* ONC discusses situations when generally accepted technical standards that could be used to achieve the objective exist, but the actor does not implement them. ONC references the examples in the proposed rule, such as an EHR developer using Consolidated-Clinical Document Architecture to receive transition of care summaries but only sending them in a propriety format.

A word of caution concerning these examples of potential information blocking: as ONC acknowledges, a practice that seems to implicate the information blocking prohibition may not necessarily constitute information blocking. For example, the practice could be required by law, fail to meet one or more elements of the definition of information blocking, or meet an information blocking Exception. Each situation requires careful consideration of the specific facts and circumstances.

THE EXCEPTIONS

ONC finalizes eight limited Exceptions for "reasonable and necessary" practices that do not constitute information blocking. The Exceptions reflect modified versions of the seven originally proposed exceptions and one additional exception. The eight Exceptions are broken into two categories: Exceptions that involve not fulfilling requests to access, exchange or use EHI, and Exceptions that involve procedures for fulfilling requests to access, exchange or use EHI.

Exceptions that Involve Not Fulfilling Requests to Access, Exchange or Use EHI

1. PREVENTING HARM EXCEPTION

ONC finalizes a modified version of its proposed Preventing Harm Exception, with changes intended to clarify the exception and better align it with HIPAA. The Preventing Harm Exception is intended to protect practices that the actor reasonably believes will substantially reduce the risk of patient harm or harm to another individual that would arise from the access, exchange or use of EHI, provided that the practice is no broader than necessary to substantially reduce the risk of harm and meets the following conditions:

- *Types of Risk*: The risk of harm being addressed must either be based on an individualized exercise of professional judgment of a licensed health care professional with a current or prior clinician-patient relationship with the relevant patient, or arise from data known or reasonably suspected of being misidentified, mismatched, corrupt or otherwise erroneous.
- *Types of Harm*: Different harm standards will apply to permissible practices involving EHI depending on the circumstance, as described in the table below.

	Type of Access, Exchange or Use that the Practice is Likely to Interfere With, or Actually Interfered With	EHI	Type of Risk	Harm Standard
1.	Access, exchange, or use by a patient's personal representative under HIPAA or other legal representative	Patient's EHI	Licensed health care professional determination of potential harm in providing access, exchange or use	Substantial harm to the patient or another person
2.	Access, exchange, or use by a patient or patient's personal representative under HIPAA or other legal representative	Information that references another person aside from the patient	Licensed health care professional determination of potential harm in providing access, exchange or use	Substantial harm to such other person referenced in the EHI
3.	Access, exchange, or use by a patient	Patient's EHI	Licensed health care professional determination of potential harm in providing access, exchange or use, or potential issues with data requested	Harm to the life or physical safety of the patient or another person
4.	Any legally permissible access, exchange or use not covered under 1–3		Licensed health care professional determination of potential harm in providing access, exchange or use, or potential issues with data requested	Harm to life or physical safety of the individual or another person

Where the risk of harm is based on the licensed health care professional's determination, in order to be protected the actor must have a practice that allows for the review and potential reversal of that determination, consistent with the individual patient's rights under the HIPAA Privacy Rule or any other federal, state or tribal law. The practice also would have to implement an organizational policy that meets a number of conditions (*e.g.*, is in writing, is based on relevant expertise, is implemented consistently and in a non-discriminatory manner, and conforms the practice to the relevant conditions of the Exception). Alternatively, the practice would have to result from a determination, based on the facts and circumstances known or reasonably believed by the actor (at the time of the determination and throughout the practice) and on relevant expertise.

2. Privacy Exception

An actor's conduct meets the Privacy Exception if it meets one of four separate sub-exceptions. ONC states that it generally intends the sub-exceptions to align the final rule with an individual's privacy rights under the HIPAA Privacy Rule, and to reflect ONC's view that the final rule should not compel actors to share EHI against patients' expectations or without adequate safeguards.

First Sub-Exception: Unsatisfied Legal Preconditions to the Release of EHI

Under the first sub-exception, an actor may withhold EHI on the basis that a state or federal privacy law imposes a precondition for providing access, exchange or use of EHI (*e.g.*, a requirement to obtain a patient's consent before disclosing the EHI), if the actor's practice is tailored to the applicable precondition, is implemented in a consistent and non-discriminatory manner, and either:

- Conforms to the actor's written, implemented policies and procedures that specify the criteria that the actor uses to determine when the precondition is satisfied and applicable steps that the actor takes to satisfy the precondition; or
- Is documented by the actor, on a case-by-case basis, in a record that identifies 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.

For example, ONC notes in the final rule preamble that, subject to the above requirements, an actor may refuse to disclose EHI if the actor is unable to reasonably verify the identity and authority of a requestor in accordance with the HIPAA Privacy Rule. ONC also states that an actor may refuse to disclose EHI concerning a patient of a federally assisted substance use disorder treatment program if the federal regulations at 42 CFR Part 2 require the patient's consent for the disclosure of the requested EHI.

If the precondition relies on the provision of a consent or authorization from an individual, and the actor has received a consent or authorization that does not satisfy all elements required by applicable law, the actor must (1) use reasonable efforts to provide the individual with a consent or authorization form that satisfies all required elements, or (2) provide other reasonable assistance to the individual to satisfy the precondition. The actor may not improperly encourage or induce the individual to withhold the consent or authorization. While the final rule does not define what constitutes an improper encouragement or inducement, ONC states in the preamble to the final rule that an actor may inform an individual about the advantages and disadvantages of exchanging EHI and any associated risks as long as the information communicated is accurate and legitimate.

Second Sub-Exception: Certified Health IT Developer Not Covered by HIPAA

A certified health IT developer that is not a HIPAA covered entity or business associate, such as a direct-to-consumer health IT provider, may meet the second sub-exception if a practice promotes the privacy interests of an individual. To meet the sub-exception the certified health IT developer's privacy policies must have been disclosed to the individuals and entities that use the actor's product or service before they agreed to use the product or service, and the developer must implemented the practice according to a process described in the privacy policies. In the preamble to the final rule, ONC states that it would be reasonable, for example, if the actor discloses its privacy policies by posting a privacy notice or otherwise describing its privacy practices on its website. ONC encourages developers to implement a transparent consumer-facing privacy policy based on its Model Privacy Notice. The actor's privacy policies also must comply with applicable state and federal laws, be tailored to the specific privacy risk or interest being addressed, and be implemented in a consistent and non-discriminatory manner.

Third Sub-Exception: Denial of an Individual's Request for EPHI Consistent with the HIPAA Privacy Rule

An actor that is a HIPAA covered entity or business associate meets the third sub-exception if an individual requests EHI under the HIPAA Privacy Rule's right of access provision and the actor's practice complies with the Privacy Rule's "unreviewable grounds" for a denial of access. The unreviewable grounds include certain requests made by inmates of correctional institutions; information created or obtained during research that includes treatment, if certain conditions are met; denials permitted by the federal Privacy Act; and information obtained from non-health care providers pursuant to promises of confidentiality.

Fourth Sub-Exception: Respecting an Individual's Request Not to Share Information

Unless otherwise required by law, the fourth sub-exception permits an actor to decline to provide access, exchange or use of an individual's EHI if it meets the following requirements, which are intended to align with an individual's right to request additional restrictions under the HIPAA Privacy Rule:

- The individual who is the subject of the EHI requests that the actor not provide such access, exchange or use of the EHI without any improper encouragement or inducement of the request by the actor;
- The actor documents the request within a reasonable time period. While the sub-exception does not define "reasonable time" nor require the request to be dated, in the final rule preamble, ONC recommends that the request be dated in order to document that the request was received before the actor declines access, exchange or use of EHI;
    - The actor's practice is implemented in a consistent and non-discriminatory manner; and
    - An actor may terminate an individual's request for a restriction to not provide such access, exchange or use of the individual's EHI only if the individual agrees to the termination in writing or requests the termination in writing, the individual orally agrees to the termination and the oral agreement is documented by the actor, or the actor informs the individual that it is terminating its agreement to not provide such access, exchange or use of the individual's EHI and certain additional requirements are met.

3. SECURITY EXCEPTION

The Security Exception allows actors to implement reasonable and necessary security practices, and prohibits security practices that could be disguised information blocking. Under the Security Exception, an actor's practice to protect the security of EHI is not information blocking if it is directly related to safeguarding the confidentiality, integrity and availability of EHI; tailored to the specific security risk being addressed; and implemented in a consistent and non-discriminatory manner. In addition, the practice must meet one of the following conditions:

- If the security practice implements an organizational security policy, the policy must:
  - Be in writing;
  - Have been prepared on the basis of, and be directly responsive to, security risks identified and assessed by or on behalf of the actor (for example, in a security risk assessment complying with the HIPAA Security Rule);
  - Align with one or more applicable consensus-based standards (such as the NIST Cybersecurity Framework) or best practice guidance; and
  - Provide objective timeframes and other parameters for identifying, responding to and addressing security incidents. In the preamble to the final rule, ONC recommends that the policy explicitly reference the applicable consensus-based standards or best practice guidance. ONC identifies the NIST Incident Response Procedure as an example of an acceptable source for the development of a security incident response plan.
- If the security practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particularized facts and circumstances, that:
  - The practice is necessary to mitigate the security risk to EHI; and
  - There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent or materially discourage the access, exchange or use of EHI.

This condition, which allows a case-by-case analysis, will be helpful where an actor needs to protect EHI against an unexpected threat that is not addressed by then-existing written security policies.

While ONC intends to align the Security Exception with the HIPAA Security Rule, it cautions in the final rule preamble that compliance with the Security Rule does not, standing alone, establish that the security measure meets the Security Exception. Instead, the security measure must achieve a balance that meets the Security Rule's requirement for reasonable and appropriate security as well as the Security Exception's requirements for avoiding unreasonable interference with access, exchange and use of EHI.

4. Infeasibility Exception

An actor's practice of not fulfilling a request to access, exchange or use EHI due to the infeasibility of the request will not be considered information blocking under the final Infeasibility Exception, provided that the actor meets one of the following three conditions and, within ten business days of receipt of the request, provides to the requestor in writing the reasons why the request is infeasible.

- *Uncontrollable Events*. The actor cannot fulfill the request for access, exchange, or use of EHI due to a natural or human-made disaster, public health

emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption or act of military, civil or regulatory authority.

- *Segmentation*. The actor cannot fulfill the request for access, exchange, or use of EHI because the actor cannot unambiguously segment the requested EHI from EHI that:
  - Cannot be made available due to an patient's preference or because the EHI cannot be made available by law; or
  - May be withheld in accordance with the Preventing Harm Exception.
- *Infeasible Under the Circumstances*. The actor demonstrates, prior to responding to the request, through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances:
  - The type of EHI and the purposes for which the EHI may be needed;
  - The cost to the actor of complying with the request in the manner requested;
  - The financial and technical resources available to the actor;
  - Whether the actor's practice is non-discriminatory and the actor provides the same access, exchange, or use of EHI to its companies 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, HIE or HIN through which EHI is accessed or exchanged; and
  - Why the actor was unable to provide access, exchange, or use of EHI consistent with the Content and Manner Exception (discussed below).

In determining whether the circumstances were infeasible under the above factors, the actor may not consider whether the manner requested would have facilitated competition with the actor or prevented the actor from charging a fee or would have resulted in a reduced fee.

5. Health IT Performance Exception

Under the Health IT Performance Exception, an actor's practice to maintain or improve health IT performance is not information blocking when the practice meets one of the following conditions:

- *Maintenance and Improvements to Health IT*. When an actor implements a practice that makes health IT under that actor's control temporarily unavailable, or that temporarily degrades the performance of health IT in order to perform maintenance or improvements to the health IT, the actor's practice must be:
  - Implemented for a period of time no longer than necessary to complete the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;
  - Implemented in a consistent and non-discriminatory manner; and

- If the unavailability or degradation is initiated by a certified health IT developer, HIE or HIN, then the practice must be either:
  - Consistent with existing service level agreements between the individual or entity to whom the certified health IT developer, HIN or HIE supplied the health IT if planned; or
  - Consistent with existing service level agreements between the individual or entity, or agreed to by the individual or entity to whom the certified health IT developer, HIN or HIE supplied the health IT if unplanned.

- *Assured Level of Performance*. An actor may take action against a third-party application that is negatively affecting the health IT's performance, provided that the practice is:
  - Implemented for a period of time no longer than necessary to resolve any negative impacts;
  - Implemented in a consistent and non-discriminatory manner; and
  - Consistent with existing service level agreements, where applicable.
    - *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 the Preventing Harm Exception at all relevant times.
    - *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 EHI, the actor does not need to satisfy the Health IT Performance Exception, but must comply with the Security Exception at all relevant times.

Exceptions that Involve Procedures for Fulfilling Requests to Access, Exchange or Use EHI

6. Content and Manner Exception

ONC establishes a new Content and Manner Exception in the final rule in an effort to address two groups of comments received on the proposed rule. Some commenters raised concerns about ONC's proposed broad definition of EHI and sought flexibility to implement compliance with the information blocking provisions. Other comments sought clarification of ONC's proposed incorporation of a "reasonable alternative" requirement in the proposed Infeasibility Exception.

The Content and Manner Exception, as the name implies, identifies the information that an actor must provide in response to a request, and the manner in which the actor must fulfill the request, if an actor seeks protection under the Exception. In essence, the Content and Manner Exception identifies permissible limitations on what information an actor provides and how an actor provides it.

Content

To be protected under the Content and Manner Exception from a content perspective, when responding to a request for access, exchange or use of EHI, the actor must respond with the subset of EHI identified by the USCDI data elements until the date 24 months after the publication of the final rule in the *Federal Register*.

After that date, actors must respond with all EHI in a designated record set as discussed above.

Manner of Response

An actor must fulfill a request for access, exchange or use of the required EHI *in the manner requested*, unless the actor cannot technically fulfill the request, or the actor and requestor are unable to reach mutually agreeable terms. If an actor fulfills a request in the manner requested, then the fee and licensing limitations in the Fee Exception and Licensing Exception, respectively, would not apply. Thus, under this scenario, the actor would have the opportunity to negotiate mutually agreeable fees and other terms with requestors that reflect market terms, without immediately subjecting the terms to the conditions of the Fee Exception and Licensing Exception.

ONC intends for this new Exception to provide "market participants the ability [to] reach and maintain market negotiated terms for access, exchange and use of EHI." Whether that will be the end result remains to be seen, as some requestors may opt to allow initial negotiations to fail in order to obtain the potentially greater leverage provided by the Fee Exception and Licensing Exception or the threat of penalties for information blocking. On the other hand, some requestors may negotiate because of the desire to receive access to requested EHI in a particular manner.

If the actor does not fulfill a request in the requested manner (due to technical infeasibility or failure to mutually agree on terms), then the actor must fulfill the request in an alternative manner without unnecessary delay. The Content and Manner Exception prescribes the following order of alternative manners for fulfilling requests, and only permits an actor to move to the next manner if the actor is unable to fulfill the request in the prior manner:

- Using ONC certified technology that the requestor specifies;
- Using requestor-specified content and transport standards published by either the federal government or an American National Standards Institute accredited standards development organization; and
- Using an alternative machine-readable format agreed to by the requestor, inclusive of the means to interpret the EHI.

When an actor fulfills a request in an alternative manner, the fees charged would also have to meet the Fees Exception or the Licensing Exception discussed below. This new Exception reflects ONC's preference that actors fulfill requests in the manner requested, or otherwise mutually agree with the requestor on the manner in which a request is fulfilled.

ONC also acknowledges that there may be instances when an actor should not be forced to provide the EHI in the manner requested. As an example, ONC notes that actors would not be required to automatically license their proprietary technology to satisfy the Exception if they are not able to reach agreeable terms with the requestor. Rather, the actor could provide access to EHI through an alternative means, although ONC acknowledges that in some limited situations, even fulfilling the request in an alternative manner could require licensing an actor's intellectual property to meet the Content and Manner Exception.

7. Fees Exception

The Fees Exception allows an actor to charge fees, including those that result in a reasonable profit margin, for accessing, exchanging or using EHI. As with the other Exceptions, the actor must meet specific conditions for protection to apply.

For example, the fee must be:

- Based on objective and verifiable criteria, uniformly applied for similarly situated people/requests;
- Reasonably related to the actor's costs;
- Reasonably allocated among all similarly situated people; and
- Based on costs not already recovered for the same instance of the service to a provider or third party.

The fee must *not* be based on:

- Competitive considerations;
- Sales, profit, revenue or other value that the requestor or other party may derive from the access, exchange or use of the EHI;
- Costs that an actor incurs because it designed or implemented health IT in non-standard ways (unless the requestor agreed to the fee associated with such implementation);
- Costs associated with intangible assets other than actual development and acquisition costs;
- Opportunity costs unrelated to the access, exchange or use of EHI; or
- Any costs leading to the creation of intellectual property if the actor charges a royalty for that intellectual property under the Licensing Exception (see below), and such royalty includes development costs of creating that intellectual property.

The Fees Exception does not permit actors to charge the following fees:

- Fees prohibited under the HIPAA Privacy Rule for individuals' requests for access to their protected health information;
- Fees based in any way on the electronic access of an individual's EHI by the individual, the individual's personal representatives or others designated by the individual (The final rule defines "electronic access" as "an internet-based method that makes EHI available at the time the EHI is requested and where *no manual effort* is required to fulfill the request" (emphasis added). So when an actor fulfils individuals' requests to send EHI to themselves or their personal representatives or others they designate, if the process requires manual effort, such as collating or assembling electronic health records from multiple systems, the definition of electronic access would not be met and the actor could charge a fee and meet the Fees Exception.)
- 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 agreed to the fee in writing at the time the EHR was acquired.

The Fees Exception also requires health IT developers that create certified API technology (Certified API Developers) to comply with the final rule's condition of certification for certified API technology. The condition of certification for APIs permits Certified API Developers to charge only three types of fees:

- Fees to API Information Sources (*e.g.*, a health care provider) to recover reasonably incurred development, deployment and upgrade costs;
- Fees to API Information Sources to recover reasonably incurred incremental costs for hosting certified API technology; and

- Fees to API Users (*e.g.*, third-party application developers) for value-added services supplied in connection with software that can interact with certified API technology as long as those services are not necessary to develop or deploy the software.

Under the condition of certification, for all of the fees, the Certified API Developer must also ensure that:

- Fees are based on objective and verifiable criteria that are uniformly applied to all similarly situated API Information Sources and API Users;
- Fees imposed on API Information Sources are reasonably related to the Certified API Developer's costs to supply certified API technology to, and if applicable, support certified API technology for, API Information Sources;
- Fees to supply and, if applicable, support certified API technology are reasonably allocated among all similarly situated API Information Sources; and
- Fees are not based on competitive considerations.

8. Licensing Exception

The eighth Exception applies to interoperability elements, which include hardware, software, technologies, rights or services that are necessary to access, exchange or use EHI and are controlled by the actor who receives a request for the EHI. An example of an interoperability element is technical information in the hands of a health IT developer that a requestor would need in order to access or use EHI within the health IT developer's system. The aim of the "interoperability elements" term and the Licensing Exception is to allow actors to retain rights to their intellectual property while still limiting the actor's ability to use such intellectual property as a barrier to accessing, exchanging or using EHI. An actor's license of an interoperability element for EHI to be accessed, exchanged or used is not information blocking when the practice meets all of the conditions discussed below.

- *Negotiating a license condition*. Upon receiving a request to license an interoperability element for the access, exchange or use of EHI, the actor must:
  - Begin license negotiations with the requestor within 10 business days from receipt of the request; and
  - Negotiate a license with the requestor, subject to the licensing conditions below, within 30 business days from receipt of the request.

The final rule does not address the implications of the actor negotiating a license agreement in good faith but failing to reach agreement with the prospective licensee within 30 business days, which is often the case when the parties are juggling multiple competing priorities. The final rule also does not address a situation where the prospective licensee attempts to run out the clock and use the final rule to create leverage in the negotiations.

However, in the final rule preamble, ONC states, "[a]s part of an information blocking investigation, ONC and OIG may consider documentation or other writings maintained by the Actor around the time of the request that indicate why the Actor was unable to meet the conditions [of the Licensing Exception]. This would not permit the Actor to be covered by the Licensing Exception, but discretion in determining whether to enforce the information blocking provision may be exercised."

Accordingly, to avoid relying on OIG's enforcement discretion in cases of protracted negotiations, actors should consider developing template license agreements with commercially reasonable terms that reduce negotiating time. Alternatively, the Content and Manner Exception allows an actor to respond to a request to license an interoperability element by

providing EHI in an alternative manner that does not require the interoperability element.

- *Licensing conditions*. The license provided for the interoperability element must meet the following conditions:
    - *Scope of rights*. The license must provide all rights necessary to enable the access, exchange or use of EHI, and to achieve the intended access, exchange or use of EHI via the interoperability element.
    - *Reasonable royalty*. If the actor charges a royalty for the use of the interoperability element, the royalty must be reasonable and comply with the following requirements:
        - The royalty must be non-discriminatory, consistent with the non-discrimination requirement below;
        - 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 EHI;
        - If the actor has licensed the interoperability element through a standards developing organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on terms consistent with those in the Licensing Exception, the actor may charge a royalty that is consistent with such policies; and
        - An actor may not charge a royalty for intellectual property if the actor recovered any development costs pursuant to the Fees Exception that led to the creation of the intellectual property.
    - *Non-discriminatory terms*. The royalty and other terms on which the actor licenses and otherwise provides the interoperability element must be non-discriminatory and comply with the following requirements:
        - The terms must be based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons and requests; and
        - The terms must not be based in any part on whether the requestor or other person is a competitor, potential competitor or will be using EHI obtained via the interoperability elements in a way that facilitates competition with the actor; or on the revenue or other value that the requestor may derive from access, exchange or use of EHI obtained via the interoperability elements.

Accordingly, the royalty or other compensation terms in the license agreement for the interoperability element may not be a revenue share based on the revenue that the licensee generates from EHI transferred through the interoperability element.

Actors will likely 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.

- *Collateral terms*. The actor must not require the licensee or its agents or contractors to do any of the following:
  - Not compete with the actor in any product, service or market;
  - Deal exclusively with the actor in any product, service or market;
  - Obtain additional licenses, products or services that are not related to, or can be unbundled from, the requested interoperability elements;
  - License, grant, assign or transfer to the actor any intellectual property of the licensee; or
  - Pay a fee of any kind whatsoever unless the fee meets the reasonable royalty requirements discussed above or the Fees Exception.
- *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 that:
  - The agreement states with particularity all information the actor claims as trade secrets; and
  - Such information meets the definition of a trade secret under applicable law.

- *Additional conditions*. The actor must not engage in any practice that has any of the following purposes or effects:
  - Impeding the efficient use of the interoperability elements to access, exchange or use EHI for any permissible purpose;
  - Impeding the efficient development, distribution, deployment or use of an interoperable product or service for which there is actual or potential demand; or
  - 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.

COMPLAINT PROCESS AND ENFORCEMENT

As required by the Cures Act, and in response to public comments to the proposed rule, ONC has developed a dedicated complaint process. Complaints submitted to ONC receive certain protections from public disclosure under the law, and ONC's new process offers the option to submit information blocking claims anonymously.

ONC is not the only potential recipient of information blocking complaints, however. The HHS Office of Inspector General (OIG) also has processes to receive and review information blocking claims, which ensures, in ONC's words, "that there is no 'wrong door' by which a complainant can submit information." ONC notes that it is actively coordinating with OIG to establish processes for sharing complaint information between the agencies. ONC also states that OIG will train its investigators to spot information blocking allegations as part of its other fraud and abuse investigations, and that OIG will implement information blocking complaint review and triage procedures. It is unclear whether such statements are designed to provide comfort that OIG is taking a thoughtful approach to its information blocking responsibilities, to send a warning message to actors, or both.

In the event that ONC or OIG investigates an information blocking claim and an actor asserts that its practice is protected by an Exception, the actor must demonstrate that the practices meets the conditions of the Exception, according to ONC. Consequently, it would be prudent for an actor to create documentation or other materials to support that it meets each element of the applicable Exception.

Ultimately, if OIG alleges that an actor violated the information blocking prohibition, the actor would face potential civil monetary penalties or "appropriate disincentives," depending on the type of actor involved. Certain actors—certified health IT developers, HINs and HIEs—face civil monetary penalties that, after adjustment for inflation, now exceed $1 million per violation. Meanwhile, the Cures Act requires OIG to refer health care providers, who are not subject to the same civil monetary penalties, to an appropriate agency for "appropriate disincentives."

Although ONC sought comment on potential disincentives in its proposed rule, it does not ultimately finalize any disincentives in the final rule. ONC states instead that it "shared all the comments received with the appropriate agencies and offices with [HHS] for consideration and subsequent rulemaking" to implement information blocking penalties for health care providers.

Notwithstanding the lack of clear penalties for health care providers, ONC indicates that all actors have until the compliance date (*i.e.*, six months after publication of the final rule in the *Federal Register*) to comply with the information blocking section of the final rule. ONC clarifies that civil monetary penalty enforcement for information blocking will not begin until established by future OIG notice and comment rulemaking. While we note that OIG currently has a notice of proposed rulemaking under review at the Office of Management and Budget that is described as a "technical modification" to align certain OIG civil monetary penalty provisions with new Cures Act civil monetary penalties authorities, OIG is likely to complete the rulemaking after the information blocking compliance date. Regardless of when OIG completes its rulemaking, ONC statements are clear that conduct occurring before the compliance date will not be subject to the information blocking civil monetary penalties.

Should OIG complete its rulemaking after the compliance date, it would seem to leave open the possibility that conduct occurring between the compliance date and the effective date of OIG's final rule could be subject to civil monetary penalties, even though the penalties would not actually be imposed until after OIG completes its rulemaking. Accordingly, actors are well advised to ensure that they are compliant by the compliance date.

NEXT STEPS

ONC's final rule will have a significant impact on a broad cross-section of the health care industry. There are several practical steps that an actor or other affected stakeholder might consider taking in response to the final rule, including, without limitation, the following:

- ☐ Determine the extent to which IT systems processing EHI can distinguish between data elements included in the USCDI and other EHI included in electronic medical records or other designated record sets for purposes of responding to requests for EHI during the 18-month period beginning on the final rule compliance date.
- ☐ Evaluate whether existing policies regarding an individual's right to access protected health information (PHI) reflect the Privacy Rule and the final rule's Exceptions for preventing harm to the patient or another person. Consider adopting a new policy regarding denial of access to prevent harms, such as death or bodily harm.
- ☐ Review existing privacy and security policies and procedures addressing access to EHI, including policies on verifying the identity and authority of persons and entities requesting EHI to determine whether they comply with the Privacy or Security Exceptions.
- ☐ Review existing privacy and security policies and procedures that address consent or authorization requirements to determine whether the procedures for responding to a consent or authorization that does not satisfy all requirements under applicable law comply with the Privacy Exception.
- ☐ Review online privacy policies and other notices disclosed to individuals relating to EHI to determine whether the policies and notices are tailored to specific privacy risks. Confirm that the actor has properly implemented compliance with the policies.
- ☐ Review policies and procedures addressing an individual's right under the HIPAA Privacy Rule to request additional restrictions on the use and disclosure of PHI to determine whether they comply with the Privacy Exception's sub-exception for an individual's request not to share EHI.
- ☐ Consider whether to update existing information security risk assessment tools, policies and practices to require consideration of whether a potential security measure is tailored to specific security risks (*i.e.*, security threat and vulnerability combinations) identified in the assessment, and whether there are reasonable alternatives that reduce risk of information blocking.
- ☐ Review existing security policies, procedures and measures concerning access to EHI by third-party requestors to determine whether they are directly responsive and tailored to security risks identified and assessed by or for the actor.
- ☐ Consider adopting a policy and procedures for evaluating and responding to potentially infeasible requests for EHI, including requests during public health emergencies or other uncontrollable events.
- ☐ Review internal or contractual service level agreement terms concerning the availability of EHI (*e.g.*, terms concerning the guaranteed period of system uptime) to confirm that they satisfy the Health IT Performance Exception.
- ☐ Identify hardware, software, and other items and services that are interoperability elements regulated by the final rule.
- ☐ Consider adopting policies and procedures for receiving and timely responding to requests for EHI or a license to an interoperability element from persons and entities other than the individual who is the subject of the EHI or the individual's personal representative.

- ☐ Determine whether pricing in existing or template agreements affecting access to EHI or licensing interoperability elements (*e.g.*, template agreements for an EHR vendor's app stores) complies with the Content and Manner Exception, the Fee Exception or the Licensing Exception.
- ☐ Review the other non-pricing terms of existing or template agreements affecting access to EHI or licensing interoperability elements to ensure that practices and agreement terms fit within a final rule Exception.
- ☐ Gather records of expenditures and other information to support pricing for APIs and other technology in connection with employing cost-based pricing.

The final rule goes into effect 60 days following the date of publication in the *Federal Register*. Please do not hesitate to contact your regular McDermott lawyer or any of the authors of this *Special Report* if you have questions or need assistance with understanding your obligations under the final rule.

CONTRIBUTORS

JAMES A. CANNATTI III
PARTNER

jcannatti@mwe.com
Tel +1 202 756 8866

DANIEL F. GOTTLIEB
PARTNER

dgottlieb@mwe.com
Tel +1 312 984 6471

KAREN S. SEALANDER
PARTNER

ksealander@mwe.com
Tel +1 202 756 8024

SCOTT A. WEINSTEIN
PARTNER

sweinstein@mwe.com
Tel +1 202 756 8671

LI WANG
ASSOCIATE

lwang@mwe.com
Tel +1 310 551 9347

McDermott
Will & Emery

mwe.com |