crowell moring

CLIENT ALERT

HHS Finalizes Sweeping Regulations on Interoperability of Health Information and Information Blocking

Mar.09.2020

Today, HHS released a Final Rule: 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program (Final Rule), implementing provisions in Title IV of the 21st Century Cures Act that impact data sharing and relationships among health care entities and with consumers. This regulation, published by the Office of the National Coordinator for Health IT (ONC), finalizes first of its kind policies for the new legal prohibition against information blocking, as well as updates to the Health IT Certification Program to enhance interoperability of electronic health information. The Proposed Rule was published in February 2019. CMS also issued a companion Final Rule on patient access and interoperability. ONC has made additional guidance available here.

The policies in the ONC Rule directly impact health care providers, developers of Certified Health IT, health information networks and exchanges. They will also impact any entity that creates, accesses, or exchanges electronic health information as part of its business model. For all Actors under the final information blocking policies, it will be crucial to develop transparent and non-discriminatory organizational policies and data governance frameworks that address the criteria set forth in the exceptions described below. We anticipate that these provisions will require updates to existing contracts and agreements that these Actors have with other health care stakeholders. Please contact Jodi Daniel at jdaniel@crowell.com or any member of our team to learn more about how your organization can prepare for compliance with the ONC Rule.

Information Blocking

The 21st Century Cures Act created a new legal prohibition against information blocking – defined as any practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information. ONC's regulation finalizes policies related to implementation and enforcement of this prohibition – including definitions of the Actors to whom the rule applies, the scope of electronic health information (EHI), practices covered by the law, and reasonable and necessary exceptions that serve as safe harbors.

Compliance with the information blocking prohibition is required for a limited set of data starting six months from the date of publication of the Final Rule (estimated September 2020), and beginning 24 months after the date of publication with respect to all EHI (estimated March 2022). However, no enforcement actions will occur until the HHS Office of the Inspector General establishes civil monetary penalties (CMPs) by future notice and comment rulemaking. ONC suggests that future rulemaking by OIG is coming to provide more additional detail regarding information blocking enforcement.

What Types of Actors Must Comply?

ONC's Final Rule streamlines and updates definitions of the types of Actors to which the information blocking provisions apply.

- **Health Care Providers**: As in the case of its Proposed Rule, the final definition still references the definition of "health care provider" in Section 3000 of the Public Health Service Act (as opposed to the definition of health care provider in the Health Insurance Portability and Accountability Act (HIPAA)). ONC notes that this choice allows the Secretary some latitude in expanding the definition over time.
- **Developers of Certified Health IT**: ONC has finalized its definition to include an individual or entity that develops *or offers* Certified Health IT – meaning that developers of other, non-certified health technology are not targets of information blocking enforcement. In general, Certified Health IT is health technology, primarily electronic health record (EHR) systems, which meet certain standards adopted by ONC. However, developers of Certified Health IT can be found in violation of information blocking with respect to non-certified products as well.
- **Health Information Networks and Exchanges (HIN and HIE)**: ONC opted to combine these two terms into a single definition and narrowed their scope. An entity is an HIN/HIE if it determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information among more than two unaffiliated individuals or entities, but only for a limited set of purposes drawn from HIPAA: treatment, payment, and health care operations. This excludes entities that only serve patients by providing individual access to EHI. ONC also clarified that HINs and HIEs must control the flow of EHI among multiple other entities, meaning that bilateral exchange between only two entities would not fall under this definition. An entity is an HIN or HIE based on the functions they engage in, regardless of how they are defined in the market. For example, a health plan (or its associated technology platform) could be an HIE or HIN if it engages in the activities described in the definition.

Intersection with HIPAA and Impact on Business Associates: All covered entities and business associates under HIPAA may be considered Actors for the purposes of information blocking. In general, HIPAA's Privacy Rule allows disclosures of individuals' protected health information for certain permitted purposes, but does not require covered entities or business associates to actually *make* those disclosures. HIPAA's Privacy and Security Rules are centered on balancing privacy considerations and security risk assessments with data portability and access as needed to support important health care stakeholder communication.

As finalized, ONC's information blocking policy limits covered entities and business associates' power to choose whether to pursue permissible uses or disclosures under HIPAA. Although nothing in ONC's Final Rule is meant to require disclosure of EHI in a way that would be impermissible under HIPAA, if an Actor is *permitted* to disclose EHI under HIPAA, then they are now *required* to do so to avoid potential information blocking violations – subject to the exceptions described below.

In addition, ONC states that the rule does not require parties to existing business associate agreements (BAAs) to act contrary to such BAA's contractual provisions – but warns that BAAs "must not be used in a discriminatory manner by an Actor to forbid or limit disclosures that otherwise would be permitted by the Privacy Rule." As an example, the ONC provides that "[t]o determine whether there is information blocking, the actions and processes . . . of the actors in reaching the BAA and associated service level agreements would need to be reviewed to determine whether there was any action taken by an actor that was likely to interfere with the access, exchange or use of EHI, and whether the actor had the requisite intent", unless an exception from information blocking applies. Beyond this statement, however, it is unclear how this would be enforced.

What is clear is that covered entities and business associates will need to examine existing agreements, policies and procedures, and business practices to consider how these may need to change in light of the information blocking rules. There will be a fine line for entities to walk between compliance with HIPAA and compliance with information blocking.

What Data is in Scope?

Electronic Health Information (EHI): ONC updated the definition of EHI to mean electronic protected health information (ePHI) as defined in HIPAA, *to the extent* that ePHI would be included in a designated record set. Consistent with HIPAA, exceptions include psychotherapy notes or information compiled in anticipation of litigation EHI can mean groups of records maintained by any Actor that is subject to the information blocking rule, not limited to covered entities as defined by HIPAA.

The definition of EHI neither includes nor excludes price information; instead, the Final Rule directs readers to the definition of ePHI in HIPAA to interpret whether price information is included in a designated record set. De-identified data is excluded from the definition of EHI.

Compliance with the information blocking rule with respect to all EHI as defined under the Final Rule is not required until 24 months from publication of the Final Rule. From 6 months after publication through the 24 month deadline, the scope of EHI subject to the information blocking prohibition will be limited to only data types described in the U.S. Core Data for Interoperability (USCDI).

What Activities are in Scope?

Information blocking relates to activities that make it more difficult for health care stakeholders to access health data. ONC has finalized definitions for terms such as “access,” “exchange” and “use,” as well as “interoperability elements” that stakeholders may need to access in order to access data. Interoperability elements are controlled by the Actor – anything ranging from a particular technology or technical specification, to intellectual property or agreements that data requestors must sign before accessing data held by an Actor. Each of these finalized terms will be important in determining whether a given practice may implicate the information blocking prohibition.

What are the Exceptions?

ONC details eight exceptions to the information blocking prohibition, but the agency has shifted its general enforcement approach to treat these exceptions as “safe harbors.” This means that failure to meet the conditions of an exception does not automatically mean a practice constitutes information blocking. A practice that fails to meet all of the conditions of an exception only means that the practice would be evaluated on a case-by-case basis, based on facts and circumstances, and not receive guaranteed protection from civil monetary penalties (CMPs) or from appropriate disincentives by HHS.

ONC added a new exception for “Content and Manner” and modified other exceptions that were proposed. The other exceptions are as follows:

- **Preventing Harm Exception – When will an Actor’s practice that is likely to interfere with the access, exchange, or use of EHI in order to prevent harm not be considered information blocking?** ONC defined the conditions that are required to be met in order to fall within this exception as follows: (a) the Actor has a reasonable belief that the practice will

substantially reduce a risk of harm to a patient another person; (b) the practice is no broader than necessary; and (c) the type of risk and harm meets ONC's criteria.

- **Privacy Exception – When will an Actor's practice of not fulfilling a request to access, exchange, or use EHI in order to protect an individual's privacy not be considered information blocking?** An Actor's practice must meet all of the requirements of at least one of the four defined sub-exceptions. The sub-exceptions are: (a) one or more federal or state preconditions for the access, exchange, or use of EHI have not been satisfied, (b) the Actor is a Certified Health IT developer that is not subject to HIPAA, (c) the patient has elected to restrict the sharing of their EHI, and (d) respecting an individual's request not to provide access, exchange, or use of EHI. Each of these sub-exceptions requires having and disclosing organizational policies to support these criteria to the individuals and entities that use the Actor's product or service before they agree to use them. We note that this exception is limited. ONC states that generally "if an actor is permitted to provide access, exchange, or use of EHI under the HIPAA Privacy Rule (or any other law), then the information blocking provision would require that the actor provide that access, exchange, or use of EHI so long as the actor is not prohibited by law from doing so...."
- **Security Exception – When will an Actor's practice that is likely to interfere with the access, exchange, or use of EHI in order to protect the security of EHI not be considered information blocking?** Actors can meet this exception if their practices are: (a) directly related to safeguarding the confidentiality, integrity, and availability of EHI; (b) the practice is tailored to specific security risks; and (c) the practice is implemented in a consistent and non-discriminatory manner. In addition, the practice must be part of an organizational security policy or be based on particularized facts and circumstances that demonstrate that the practice is necessary to mitigate a security risk and that there are no reasonable and appropriate alternatives to the practice.
- **Infeasibility Exception – When will an Actor's practice of not fulfilling a request to access, exchange, or use EHI due to the infeasibility of the request not be considered information blocking?** To meet the requirement for this exception, the practice must be infeasible (a) due to uncontrollable events such as public health emergencies, war, etc.; (b) the Actor does not have the ability to segment the requested EHI from EHI that cannot be disclosed due to the individual's preference or legal restrictions; or (c) the Actor has determined that the request was infeasible after evaluating the factors described in the rule in a consistent and non-discriminatory manner.
- **Health IT Performance Exception – When will an Actor's practice that is implemented to maintain or improve health IT performance and that is likely to interfere with the access, exchange, or use of EHI not be considered information blocking?** The Actor's practices must be related to the maintenance and improvement of health IT (e.g. temporary unavailability of data or degradation of the performance of health IT.) These practices must last no longer than necessary.
- **Content and Manner Exception – When will an Actor's practice of limiting the content of its response or the manner in which it fulfills a request to access, exchange, or use EHI not be considered information blocking?** Under this new exception, an Actor's practice of limiting the content of its response or the manner in which it fulfills a request to access, exchange, or use EHI will not be considered information blocking if the practice meets both a "content condition" and "manner condition." Under the content condition, an Actor may respond to a request to access, exchange, or use EHI with a set of EHI limited to the data elements in the USCDI standard for 18 months following the Final Rule's compliance date (i.e., between months 6 and 24 after publication). Under the manner condition, an Actor must respond in the manner requested unless technically unable to respond or agreeable license terms cannot be reached, in which case it must respond in an alternative manner based on an order of priority specified in the Final Rule, as well as provide the

means for the requestor to interpret the EHI, as agreed upon with the requestor. As stated above, this exception was not included in the Proposed Rule.

- **Fees Exception – When will an Actor's practice of charging fees for accessing, exchanging, or using EHI not be considered information blocking?** Under the Fees Exception, Actors may recover certain costs reasonably incurred for the access, exchange, or use of EHI that ONC believes are unlikely to present information blocking concerns. Fees may result in a reasonable profit. To meet this exception, fees must meet a number of conditions (e.g., be based on objective and verifiable criteria applied uniformly to similarly situated classes of persons or entities and requests) and must not be based on certain prohibited factors (e.g., whether the requestor is a competitor). If an Actor is a health IT developer, the Actor must also comply with all relevant conditions of certification. The exception excludes certain fees, such as specific fees based on electronic access to EHI by the individual.
- **Licensing Exception – When will an Actor's practice to license interoperability elements in order for EHI to be accessed, exchanged, or used not be considered information blocking?** According to the Licensing Exception, an Actor practice to license interoperability elements for EHI to be accessed, exchanged, or used will not be considered information blocking if the practice meets certain timing requirements and licensing conditions. The Actor must begin license negotiations with the requestor within 10 business days from receipt of the request and negotiate a license within 30 business days from receipt of the request. Royalties and terms of the license also generally must be reasonable and non-discriminatory, in accordance with specified licensing conditions.

Health IT Certification Program

The ONC Final Rule also updates the ONC's Health IT Certification Program, which sets a baseline standard for functionality of health IT software, primarily electronic health records. Notable policy updates include:

- Adoption of the USCDI standard to replace the Common Clinical Data Set (CCDS) as the default set of data categories that health IT users should expect to be able to exchange between systems.
- Inclusion of Clinical Notes, Data Provenance, and EHI Export as required data categories for exchange as part of the USCDI. However, EHI Export will not be part of the Base EHR definition.
- Updates to certification requirements for application programming interfaces (APIs):
    - *Conditions of Certification*: The 21st Century Cures Act mandated that Certified Health IT be able to provide access to "all data elements" of a patient's record and allow this data to be accessed "without special effort." In furtherance of this mandate, Certified API Developers must publish complete business and technical documentation through a publicly accessible hyperlink, ostensibly reducing the need for additional effort in order for third parties to figure out how to connect. Terms and conditions for use of API technology should include any fees, restrictions, limitations, obligations, registration process requirements, or other similar requirements.
    - *Technical Updates*: ONC has finalized the FHIR Release 4.0.1 standard as the requirement for certified APIs. While some commenters urged ONC to require "write" functionality as well as "read," ONC declined to do so at this time, stating that "write" services have not yet reached maturity, but urging the industry to continue piloting "write" applications for consideration in future rulemaking.
    - *Application Registration and Vetting*: Applications must register with an authorization server; but this is a basic technical requirement, not a review process for privacy, quality, or any other substantive criteria. ONC has

clarified that any practice of reviewing third party applications must not violate information blocking, and made it clear that Certified Health IT developers cannot institute any vetting process for applications that are facilitating patient access to EHI. In response to comments about security concerns, ONC stated that the implementation of technical specifications such as OpenID Connect and OAuth 2.0 allow for secure API deployment, and that otherwise "there is little protection software can provide to protect against nefarious Actors posing as legitimate health facilities."

- Adoption of the Real World Testing certification criteria for health IT developers with Health IT Modules certified to one of more of the certification criteria focused on interoperability and data exchange or availability. Rather than requiring health IT developers to use a specific "one size fits all" set of testing tools, ONC provided a framework of topics and considerations that every developer must address in the required real world testing plans. Developers must include a metric for each of the certification criteria that apply to their health IT modules and must work with the ONC-ACB to determine when the testing plans must be submitted in order for the ONC-ACB to complete its review and publish the plan no later than December 15 of each year.
- Adoption of a Condition of Certification that protects communications related to certain protected subject areas. Health IT developers are prohibited from restricting communications that are related to:
    - The usability of the health information technology;
    - The interoperability of the health information technology;
    - The security of the health information technology;
    - Relevant information regarding users' experiences when using the health information technology;
    - The business practices of developers of health information technology related to exchanging electronic health information; and
    - The manner in which a user of the health information technology has used such technology.

  Communications that include information about prices and costs of health IT and information regarding timelines, terms, IT workarounds, and customizations is also protected communication. The rule provides that users may publish screenshots or video of health IT, so long as they are unaltered and are limited in number (screenshots) or length (video) to communicate about one or more of the six protected subject areas.

  As of the effective date, developers may not engage in conduct that would have the effect of prohibiting or restricting protected communications and must include provisions that do not contravene this Condition of Certification's requirements in new or amended contracts.

* * *

The Final Rule is wide-ranging in its implications for organizations across the health care industry. For further guidance on how your organization can prepare for compliance, please contact our team.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Jodi G. Daniel
Partner – Washington, D.C.
Phone: +1 202.624.2908
Email: jdaniel@crowell.com

Brandon C. Ge
Counsel – Washington, D.C.
Phone: +1 202.624.2531
Email: bge@crowell.com