CLIENT ALERT

ONC Proposes Regulations on Health IT Certification and Information Blocking

February 12, 2019

The Office of the National Coordinator for Health Information Technology (ONC) has released a proposed rule implementing key provisions in the 21st Century Cures Act (Cures Act) governing health IT certification and information blocking, and other issues intended to advance interoperability and support the access, exchange, and use of electronic health information (EHI). The proposed rule aligns with CMS' new regulation implementing the Cures Act provisions, released concurrently.

Provisions in these rules regarding information blocking and API access to data are expected to have a transformative impact on interoperability and the way data is exchanged between patients, providers, plans, technology developers, and other health care stakeholders. The proposed rule is also expected to facilitate improved patient access, price transparency, and the use of value added tools to improve health care delivery and health outcomes.

Comments are due 60 days after publication in the Federal Register.

What does the proposed rule say about information blocking?

The general prohibition on information blocking applies to health care providers, developers of certified health IT, health information exchanges, and health information networks. The Cures Act defines information blocking broadly as any practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information (EHI) when the entity knows it is likely to do so.

In the proposed rule, ONC: (1) defines key terms, including EHI; (2) provides an illustrative list of activities that would be likely to interfere with access, exchange, or use of EHI; (3) codifies compliance with the information blocking provisions as a Condition of Certification; (4) introduces seven exceptions to the general prohibition on information blocking; and (5) issues a Request for Information on disincentives for health care providers.

Definition of EHI

The proposed rule's definitions would establish the scope of who and what is covered by the information blocking provisions and are key to understanding the rules. The Cures Act fails to define key terms such as "electronic health information" or "EHI," "network," and "exchange," so ONC has proposed definitions. The proposed rule relies on the definition of "health information" from HIPAA and defines EHI broadly as:

1. Electronic protected health information; and
2. Any other information that
    - Is transmitted by or maintained in electronic media, as defined in 45 CFR § 160.103;

  - Identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
  - Relates to the past, present, or future health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

The definition of EHI is similar, but not identical, to the definitions of protected health information (PHI) and electronic protected health information (ePHI) used in the Health Insurance Portability and Accountability Act and its implementing regulations (HIPAA). The definitions of PHI and ePHI are limited to health information created or received by HIPAA covered entities and certain others. Therefore, for example, information in many direct-to-consumer health-related applications are not subject to HIPAA. EHI, on the other hand, is broader and includes health information provided directly from an individual to an entity subject to the information blocking provisions. The proposed rule also excludes information that is de-identified consistent with HIPAA requirements from the definition of EHI.

ONC' proposed definition of EHI is expansive and includes information on an individual's health insurance eligibility and benefits, billing for health care services, and payment information for services to be provided or already provided, which may include price information.

With the growing importance of price information, ONC also seeks comment on whether to include price information in the definition of EHI in an effort to promote price transparency.

Definitions of Network and Exchange

The terms "network" and "exchange" are not defined in the Cures Act but are critical as they determine who is subject to the information blocking prohibition.

ONC has defined these terms in a way that does not assume the application or use of certain technologies and is intended to apply to the full range and diversity of exchanges and networks that exist today and may arise in the future. ONC's definition of "health information network" (HIN) focuses on the role of these actors in the health information ecosystem. Specifically, an entity is an HIN if it: (1) determines, oversees, administers, controls, or substantially influences policies or agreements that define the business, operational, technical, or other conditions or requirements that enable or facilitate the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities; or (2) provides, manages, controls, or substantially influences any technology or service that enables or facilitates the access, exchange, or use of EHI between or among two or more unaffiliated individuals or entities.

"Health information exchange" (HIE) on the other hand is more narrowly defined as an individual or entity that enables access, exchange, or use of EHI primarily between or among a particular class of individuals or entities or for a limited set of purposes.

Examples of Practices Likely to Interfere with Access, Exchange, or Use of EHI

To clarify the scope of the information blocking provision, the proposed rule outlines several types of practices that ONC believes are likely to interfere with access, exchange, or use of EHI. The examples include:

- Restrictions on access, exchange, or use of EHI through formal means (e.g., contractual restrictions) or informal means (e.g., ignoring requests to share EHI).
- Limiting or restricting the interoperability of health IT (e.g., disabling a capability that allows users to share EHI with users of other systems).
- Impeding innovations and advancements in access, exchange, or use or health IT-enabled care delivery (e.g., refusing to license interoperability elements to others who require such elements to develop and provide interoperable services).
- Rent-seeking and other opportunistic pricing practices (e.g., charging fees to provide interoperability services that exceed actual costs incurred to provide the services).
- Non-standard implementation practices (e.g., choosing not to adopt relevant standards, implementation specifications, and certification criteria).

Exceptions

The proposed rule sets forth seven "reasonable and necessary" activities that do not constitute information blocking under certain conditions:

1. **Engaging in practices that prevent physical harm** to a patient or another person in certain narrowly defined circumstances. Examples include, risk of corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record, risk of misidentifying a patient or patient's electronic health information, or determination by a licensed health care professional that the disclosure of EHI is reasonably likely to endanger life or physical safety.
2. **Engaging in practices that protect the privacy of EHI**, consistent with applicable law, including HIPAA and Part 2. For example, not providing access, exchange, or use of EHI when a state or federal law requires that a condition be satisfied before an actor provides access, exchange, or use of EHI, and the condition is not satisfied or not sharing EHI against patients' wishes.
3. **Implementing measures to promote the security of EHI,** whereby the practice is directly related to safeguarding the confidentiality, integrity, and availability of EHI and narrowly tailored.
4. **Recovering costs reasonably incurred** in providing access, exchange, or use of EHI, subject to strict conditions. ONC would require that the costs the actor recovered were reasonably incurred and not speculative or subjective and that costs are allocated objectively. ONC would prohibit certain fees, such as those based on the profit or revenue associated with the use of EHI that exceed the actor's reasonable costs for providing access, exchange, or use of the EHI.
5. **Declining to provide access, exchange, or use of EHI if a request is infeasible,** such as where complying with the request would impose a substantial burden on the actor.
6. **Licensing technologies or other interoperability elements that are necessary to enable access to EHI.** The terms must be reasonable and non-discriminatory and the actor, if a health IT developer, must comply with all conditions of certification discussed below.
7. **Making health IT unavailable to perform maintenance or improvements,** both planned and unplanned**.** For example, services level agreements that provide flexibility for maintenance is allowed if conditions are met.

Disincentives

In the proposed rule, ONC also requests information on disincentives or if modifying disincentives already available under other HHS programs and regulations would more effectively deter health care providers from engaging in information blocking.

What does the proposed rule say about health IT certification?

ONC proposes a number of changes to the ONC Health IT Certification Program through deregulation and updates to the 2015 Edition Certification Criteria.

In order to reduce burden on providers and health IT developers, ONC proposes six deregulatory actions that would scale back the ONC Health IT Certification Program (Program) and asked that commenters identify any additional deregulatory actions that the Office may consider. These actions include the development of exemptions to ONC Program requirements for health IT developers holding precertification under the FDA's Software Precertification Program.

Adoption of the United States Core Data for Interoperability (USCDI) Standard

ONC proposes the removal of the 2015 Edition "Common Clinical Data Set" (CCDS) in favor of the adoption of the USCDI—a standard that will specify a common set of data classes for interoperable exchange. These data classes would comprise the existing code sets within CCDS as well as two new data classes: "clinical notes," which includes eight types of clinical notes as the minimum standard, and "provenance," which allows stakeholders to assess the reliability of the data.

Conditions and Maintenance of Certification

ONC also proposes an approach whereby health IT developers must attest to initial certification requirements and meet ongoing Conditions to remain under the Program. The Conditions include: (1) a prohibition on developer actions that constitute information blocking; (2) permitted prohibitions and restrictions on communications regarding health IT; (3) standards, specifications, and criteria for APIs; and (4) real world testing for interoperability.

Information Blocking

The proposed rule would establish, as a Condition of Certification for the ONC Health IT Certification Program, that a health IT developer must provide satisfactory assurances that it will not take any action that constitutes information blocking unless it falls under an exception. As part of such assurances, a health IT developer must meet various administrative requirements, including maintaining records of initial and ongoing compliance.

Communications

ONC acknowledges current developer practices that limit health IT users from openly discussing or sharing their experiences with health IT and proposes a new Condition of Certification that would protect certain communications and communicators. Health IT developers would be precluded from prohibiting or restricting any communication, irrespective of the form of the communication or the identity of the communicator, if the communication is within the range of "protected subject areas."

ONC notes that developers prohibit or restrict communication through contract, such as non-disclosure agreements or other contractual terms, and conduct, including punitive or retaliatory actions against the users of health IT. For the Condition of

Certification to be implicated, the developer's conduct must have a nexus to the making of, or attempted or contemplated making of, a protected communication.

ONC defines "protected subject areas" as those that implicate

- A health IT technology's usability, interoperability, or security.
- The manner in which the users have used the technology.
- The users' experience.
- Any business practices of health IT developers related to the exchange of EHI.

Health IT developers would also be prohibited from imposing *any* prohibitions or restrictions on a narrow class of communications ("unqualified protections").

Health IT developers would be permitted to impose narrow prohibitions on communications that:

- Are made by their own employees.
- Disclose non-user-facing aspects of the software.
- Infringe on the developers intellectual property rights, so long as the communication was not made in "fair use" of the health IT.
- Are unfaithful reproductions of health IT screenshots.
- Are made during "beta" testing or unreleased product development.

ONC's proposal seeks to improve transparency around the functioning of health IT while balancing the developers' need to protect their legitimate interests.

APIs

ONC is proposing a new API certification criterion at 170.315(g)(10), to effectively replace the 2015 criterion (g)(8) that allowed access to each of the data categories in the CCDS (other API criteria, such as (g)(7) and (g)(9) remain as is). The new (g)(10) requirement will support two use cases: patient access to their own data, and population level access to a group of patients' data (such as a provider's patient panel, or all patients under a particular health plan). The core functionality currently required is "read" and not "write," meaning that for now applications will be able to pull data but not push it back up to the EHR – although ONC envisions requiring "write" functionality in the future. APIs must offer the following functionalities: data response; search support; app registration; secure connection, authentication and authorization (leveraging OpenID Connect Core). Patients should be able to get "persistent access" to their health information without having to re-authenticate for a proposed minimum period of three months.

- Standard: As expected and given its wide adoption in the market, ONC proposes to use FHIR as the underlying standard to enable API access.
- Data Elements: Vendors would make available a certain set of FHIR resources that correspond to the USCDI, named API Resource Collection in Health (ARCH).

- Transparency: Vendors would make publicly accessible their API technical documentation, including implementation specifications and information about any unique technical requirements required for access. Documentation must be publicly available via a hyperlink, and cannot be behind a paywall or any type of registration requirement.
- Conditions of Certification: Vendors would be required to make their business documentation transparent as well. Specifically, vendors' terms and conditions, including fees, registration process requirements, and any limitations or obligations of application developers would need to be openly published via a public hyperlink.
- Fees: ONC proposes a general prohibition on imposing fees associated with API technology, unless the fee arrangement falls within a specific permitted category. Permitted fees must be based on objective and verifiable criteria, uniformly applied across applications vying for API access, and must be reasonably related to the cost of supplying, maintaining, and upgrading the API. Fees may not be predicated on an application's status as a competitor to the vendor. Any usage fee associated with patient access is prohibited. ONC also notes that the increasing incidence of revenue-sharing or royalty agreements would bear no relationship to costs incurred, and are likely to run afoul of the regulation.
- Intellectual Property and Right to Access: Vendors would need to grant API users all rights that are reasonably necessary to access and use API technology in a production environment. Users should not have to pay a fee in order to license the rights to use the API, nor submit to any provisions regarding exclusivity or limiting competition.

Real World Testing

ONC proposes a new Condition of Certification that requires health IT developers to annually submit real world testing plans and retrospective test results that include interoperability criteria. ONC describes the objective of the testing to verify that the health IT continues to be compliant with certification criteria, is exchanging EHI in the care and practice settings for which it is intended, and EHI is received and used by the technology.

Requests for Information

Price Transparency and Information Blocking

In the Notice of Proposed Rule Making (NPRM), HHS states its interest in subsequent rulemaking to expand access to price information for the public, prospective patients, plan sponsors, and health care providers, and includes a series of questions on how best to do this. The stated concern is that the fragmented and complex nature of pricing for health care has negative effects, including increasing out-of-network costs and surprise billing, and that price transparency can help patients and promote competition. Furthermore, HHS noted ONC's role in establishing the framework to prevent the blocking of price information, suggesting that its authority is broad enough to cover payer-provider networks and benefits, coverage, and price information. The NPRM poses questions about how to define and implement price transparency.

TEFCA

Under the Cures Act, ONC was charged with developing a trusted exchange framework, including a common agreement among health information networks. Following up on ONC's draft Trusted Exchange Framework and Common Agreement (TEFCA) from last year, ONC also issued a request for information regarding a proposal for a new Condition of Certification that would require health IT developers to participate in TEFCA to assure that they do not take any actions that would constitute information blocking. ONC states that existing certification criteria for the Certified Health IT program require developers to attest to their capabilities to provide access and exchange of EHI. Therefore health IT developers that have a Health IT Module with capabilities that support access and exchange of EHI would be best suited to participate in TEFCA and in a position to provide connection services to HINs.

ONC asks for comments regarding the certification criteria identified as the basis for the participation of health IT developers in TEFCA, as well as whether TEFCA, in its current structure, is conducive to health IT developer participation.

Other requests for information

The proposed rule also contains requests for information on registries, patient matching (i.e., linking a patient's data within and across health care providers), and how certification and emerging technology can support efforts to reduce and treat opioid abuse.

Next steps

ONC seeks comment on the proposed rule by mid-April. Crowell & Moring's Digital Health team is here to help your organization understand and respond to the proposed rule.

In addition, ONC anticipates issuing another draft version of the TEFCA in the coming months. Stakeholders should consider their response to the TEFCA provisions of the ONC rule, as well as identify existing issues with TEFCA to prepare for the forthcoming update.

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

Jodi G. Daniel
Partner & CHS Managing Director – 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