Executive Summary of Final Rule

Background

In December 2016, the landmark *21st Century Cures Act* was signed into law. Many of the provisions in the law focused on improving interoperability of health information, including Sec. 4004, which forbids the practice of information blocking.

Sec. 4004 defines information blocking as a practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information, and requires the Secretary of Health and Human Services, through rulemaking, to identify reasonable and necessary activities that do not constitute information blocking. The Final Rule, released on March 9 by the Office of the National Coordinator for Health IT (ONC) and entitled *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program*, carries out this statutory directive, in addition to finalizing related updates and changes to the ONC Voluntary Certification Program for Health IT.

The rule is in two parts: the first finalizes changes to the Health IT Certification Program, which is a voluntary certification program for health information technology products. The second finalizes definitions of what data must be exchanged in order to avoid violating the statute, who is subject to information blocking enforcement actions, and reasonable and necessary activities that do not constitute information blocking (i.e.: exemptions).

Key Takeaways from Final Rule

- ONC is moving forward with policy that requires actors to make electronic health information (EHI) available to patients – and any entity of their choosing, including third-party applications – via a certified application programming interface (API)
- In response to concerns from the public and healthcare stakeholders that data will lose crucial privacy and security protections once it leaves a HIPAA covered entity and goes to a third-party application (that often is not subject to HIPAA), ONC states:
    - That it supports an individual's ability to choose which third-party developer and app are best for receiving their EHI from a health care provider, as well as an individual's ability to agree to the third-party developer or app's terms of use
    - That it also supports and strongly encourages actors providing individuals with information that will assist them in making the best choice for themselves in selecting a third-party app.

        - Specifically, ONC writes that "Individuals concerned about information privacy and security can gain a better understanding about how the third-party apps are using and storing their EHI, how individuals will be able to exercise any consent options, and more about what individuals are consenting to before they allow the app to receive their EHI." Notably, this appears to put the onus for educating individuals about potential privacy and security risks on the disclosing actor.
    - Security should not be a concern for the *disclosing actor's health IT systems* if the actor is using a certified API, because the apps would only be able to receive EHI at the patient's direction

- In response to many comments on the proposed rule objecting to its broad definition of EHI – which went beyond the HIPAA definition of electronic patient health information (ePHI) – ONC significantly narrowed the definition of EHI in the final rule to align with the HIPAA ePHI definition

- ONC finalized eight exemptions to information blocking, specifically for reasons involving:
    - Preventing harm
    - Privacy
    - Security
    - Infeasibility
    - Health IT performance
    - Content and manner
    - Fees
    - Licensing

- ONC finalized a requirement that health IT developers must not prohibit or restrict communications about certain aspects of the performance of health IT and the developers' related business practices, including the sharing of screenshots and/or videos
    - Despite the comments of some health IT developers to the proposed rule that sharing screenshots could expose their intellectual property (IP, ONC finalized its original proposal to allow screenshots and/or videos of screens, with the caveat that health IT developers can limit sharing based on the doctrine of "fair use"

- Deadlines for complying with the provisions of the Final Rule vary – find a timeline from ONC HERE
    - Although compliance with the information blocking provisions must happen within six months of publication in the Federal Register of the Final Rule, imposition of civil monetary penalties will not begin until future rulemaking by the Office of the Inspector General

Attached please find a more detailed summary of the Final Rule.

Detailed Summary of Final Rule

Certification of Health IT

Changes to 2015 CEHRT

- Finalized USCDI as the minimum baseline of data classes that are available for interoperable exchange
- Adopted NCPDP SCRIPT for e-prescribing to align with CMS regulations
- Also adopted the same electronic Prior Authorization (ePA) request and response transactions supported by the NCPDP SCRIPT standard proposed by CMS
- Removed HL7 Quality Reporting Document Architecture (QRDA) standard requirements and instead requires Health IT Modules to support the CMS QRDA Implementation Guide – removes certification requirements that do not support quality reporting for CMS programs
- Refined the scope of data a Health IT Module must export and aligned the criterion to the definition of EHI
- Adopted a new API certification criterion to replace the "application access – data category request" certification criterion
    - The new "standardized API for patient and population services" certification criterion focuses on supporting two types of API-enabled services:
        - Services for which a single patient's data is the focus
        - Services for which multiple patients' data are the focus
    - Uses HL7 FHIR standard Release 4
- Adopted two new privacy and security criteria requiring transparency attestations from developers of certified health IT
    - Will serve to identify whether or not certified health IT supports encrypting authentication credentials and/or multi-factor authentication
- Updated requirements for "data segmentation for privacy" (DS4P) certification criteria to support security tagging at the document, section, and entry levels

Modifications to the ONC Health IT Certification Program

- Finalized corrections to the 2015 Edition privacy and security certification framework
- Finalized corrections to the current Certification Companion Guides (CCGs)
- Adopted new and revised Principles of Proper Conduct (PoPC) for ONC-ACBs
- Finalized clarification that the records retention provision includes the "life of the edition" as well as three years after the retirement of an edition related to the certification of Complete EHRs and Health IT Modules
- Finalized revisions to the PoPC to clarify the basis for certification, including to permit a certification decision to be based on an evaluation conducted by the

ONC-ACB for Health IT Modules' compliance with certification criteria by use of conformity methods approved by the National Coordinator
- Finalized requirement ONC-ACBs accept test results from any ONC-Authorized Testing Laboratory in good standing under the Program and compliant with ISO/IEC 17025 accreditation requirements

Health IT for the Care Continuum

- In the final rule, ONC identified the existing 2015 CEHRT criteria and the new or revised criteria that support the voluntary certification of health IT for pediatric care and pediatric settings

Conditions and Maintenance of Certification Requirements

- Adopted the information blocking Condition of Certification requirement as proposed – prohibits any health IT developer under the Program from taking any action that constitutes information blocking as defined by section 3022(a) of the PHSA
- Finalized several Conditions of Certification and accompanying Maintenance of Certification requirements to provide assurances to the Secretary that, unless for legitimate purpose(s) as specified by the Secretary, the developer will not take any action that constitutes information blocking or any other action that may inhibit the appropriate exchange, access, and use of EHI
- Adopted more specific Conditions and Maintenance of Certification requirements to provide assurances
- The law requires a Condition and Maintenance Certification requirement under the Program that health IT developers do not prohibit or restrict communications about certain aspects of the performance of health IT and the developers' related business practices
    - Finalized provisions that allow health IT developers certified under the Program to place limitations on certain types of communications, including screenshots and video
        - Allows developers to limit the sharing of screenshots to only the relevant number needed to communicate about health IT
        - Developers can impose restrictions on the communication of screenshots that contain PHI
        - Communicators of screenshots must not alter the screenshots
        - Developers can limit sharing of screenshots – ONC has retained the concept of "fair use" as it applies to all health IT developer intellectual property under "permitted prohibitions and restrictions" – it must pass a two-part test:
            - First, the communication that is being prohibited or restricted must not fall within a class of communications that is considered to always be legitimate or reasonable – such as communications required by law, made to a government

agency, or made to a defined category of safety organizations
        - Second, to be permitted, a developer's prohibition or restriction on communications must also fall within a category of communications for which it is both legitimate and reasonable for a developer to limit the sharing of information about its health IT
    - A health IT developer must not impose or enforce any contractual requirement that contravenes the requirements of this Condition of Certification
    - If a health IT developer has contracts/agreements that contravene the requirements of this Condition of Certification, the developer must notify all affected customers, other persons, or entities that the prohibition or restriction within the contract/agreement will not be enforced by the health IT developer
- Adopted new standards, new implementation specifications, a new certification criterion, and modified the Base EHR definition to meet statutory API requirements
- Established real world testing Condition and Maintenance of Certification requirements, which apply to health IT developers with one or more Health IT Module(s) certified to specific certification criteria focused on interoperability and data exchange
    - Health IT developers must submit publicly available annual real-world testing plans as well as annual real-world testing results for these criteria
    - Under Standards Version Advancement Process (SVAP), developers will have the option to update their health IT that is certified to this criteria or use more advance version(s) of the adopted standard(s) or implementation specification(s) included in the criteria, provided such versions are approved by the National Coordinator for use in health IT certified under the Program
    - Health IT developers presenting health IT for initial certification to one of these criteria would have the option to certify to National Coordinator-approved newer version(s) of one or more of the Secretary-adopted standards or implementation specifications applicable to the criterion
    - All developers voluntarily opting to avail themselves of the SVAP flexibility must ensure that their annual real-world testing plans and real-world testing results submissions address all the versions of all the standards and implementation specifications to which each Health IT Module is certified
    - Health IT developers that wish to avail themselves of the SVAP flexibility must notify both their ONC-ACB and their affected customers of their plans to update their certified health IT, and the update's anticipated impact on their existing certified health IT
    - Added new PoPC for ONC-ACBs that requires ONC-ACBs to review and confirm that each health IT developer with one or more Health IT Module(s) certified to any one or more of the exchange criteria submits real-world testing plans and real-world results on a timeframe that allows for the ONC-ACB to confirm completeness of all plans and results by applicable annual due dates

    - Added to PoPC requirement that ONC-ACBs aggregate and report to ONC no less than quarterly all updates successfully made to support National Coordinator-approved newer versions of Secretary-adopted standards in certified health IT pursuant to the developers having voluntary opted to avail themselves of the SVAP flexibility
    - Require ONC-ACBs to ensure that developers seeking to take advantage of the SVAP flexibility provide advance notice to all affected customers and its ONC-ACB
- The Cures Act requires that a health IT developer, as Condition and Maintenance of Certification requirements under the Program, provide to the Secretary an attestation to all of the other Conditions of Certification required in the law, except for the "EHR reporting criteria submission"
    - Developers will be required to attest twice a year – submitted to the ONC-ACBs, then made publicly available through the CHPL
- ONC has yet to develop a reporting criterion as required by the Cures Act – once the program is established, ONC will undertake rulemaking and implement the associated Condition and Maintenance of Certification requirements for health IT developers
- Finalized proposed corrective action process for ONC to review potential or known instances where a Condition or Maintenance of Certification requirement under the Program has not been met or is not being met by a health IT developer – will use the ONC direct review of certified health IT in the enforcement

Information Blocking

- The Cures Act requires ONC to define actions that do ***not*** constitute information blocking. ONC was guided by three overall policy considerations in forming exceptions:
    - Exceptions are limited to certain activities that ONC believes are important to the successful functioning of the US health care system, including promoting public confidence in health IT infrastructure by supporting the privacy and security of EHI, and protecting patient safety and promoting competition and innovation in health IT and its use to provide health care services to consumers
    - Each exception is intended to address a significant risk that regulated individuals and entities will not engage in these reasonable and necessary activities because of potential uncertainty regarding whether they would be considered information blocking
    - Each exemption is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt
- ONC has finalized eight exceptions – find an overview of definitions HERE
- Failure to meet the conditions of an exception does not automatically mean a practice constitutes information blocking – it is instead evaluated on a case-by-

case basis to assess the specific facts and circumstances to determine whether information blocking has occurred

- Actors subject to information blocking enforcement:
  - Health care provider: The definition of health care provider as established by Sec. 3000 (3) of the Public Health Service Act
  - Health IT developers of certified health IT: An individual or entity that develops or offers certified health IT
    - If a developer offers *any* certified product at the time of the information blocking complaint, it could be subject to information blocking enforcement – not just on products that are certified
    - Excludes health care providers who self-develop health IT for their own use
  - Health Information Networks and Health Information Exchanges
    - Combining the definitions of HIN and HIE to create one functional definition – an individual or entity that 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 EHI: (1) among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and (2) that is for a treatment, payment, or health care operations purpose
    - Not limited to individuals or entities that are covered entities or business associates under HIPAA
- Definition of electronic health information (EHI)
  - The proposed rule adopted a broad definition of EHI – outside of what is included in the definition of ePHI, which received backlash
  - In the final rule, ONC narrowed the definition of EHI to align with the definition of ePHI under HIPAA
  - Also added an exception that allows an actor to provide, at a minimum, a limited set of EHI comprised of the data elements included in the USCDI for access, exchange, and use during the first 18 months after the compliance date of the information blocking provisions (24 months after publication of the final rule)
  - There was discussion of whether to include price information in the definition of EHI – by limiting to definition of ePHI, it would not include price information unless it is included in a designated record set
  - The definition of EHI also does not specifically include or exclude algorithms or processes that create EHI or clinical interpretation or relevancy of the results of the algorithms or processes – any such information could be considered EHI if it was ePHI included in the designated record set
  - Also, in accordance with HIPAA, de-identified information is not considered EHI
- Interests promoted by the information blocking provision
  - To meet statutory definition of information blocking, a practice must be likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI

        - Definition of access – the ability or means necessary to make EHI available for exchange, use, or both
        - Definition of exchange – the ability for electronic health information to be transmitted between and among different technologies, systems, platforms, or networks
        - Definition of use – the ability for EHI, once accessed or exchanged, to be understood and acted upon
- What vetting is permitted by actors for third-party apps
    - For certified API technology, there should be few, if any, security concerns about the risks posed by patient-facing apps to the disclosing actor's health IT systems (because the apps would only be permitted to receive EHI at the patient's direction)
    - For third-party apps chosen by the individuals to facilitate their access to their EHI held by actors, there would generally not be a need for "vetting" on security grounds and such vetting actions otherwise would be an interference – distinguishes vetting from verifying an app developer's authenticity under the API Condition of Certification
    - Actors, such as health care providers, do have the ability to conduct whatever "vetting" they deem necessary of entities (app developers) that would be their business associates under HIPAA before granting access and use of EHI to the entities – this is required by the HIPAA Security Rule
    - Allowing actors to provide additional information to individuals about apps will assist individuals as they choose apps to receive their EHI and such an approach is consistent regarding informing individuals about the advantages/disadvantages of exchanging EHI and any associated risk
        - Practices that purport to educate patients about the privacy and security of practices of apps and parties to whom a patient chooses to receive their EHI may be reviewed by OIG or ONC, as applicable, if there was a claim of information blocking
        - The information provided by actors must focus on any current privacy and/or security risks posed by the technology or the third-party developer of the technology
        - The information must be factually accurate, unbiased, objective, and not unfair or deceptive
        - The information must be provided in a non-discriminatory manner
        - An actor may not prevent an individual from deciding to provide its EHI to a technology developer or app despite any risks noted regarding the app itself or third-party developer

Enforcement

- ONC is solely responsible for enforcing compliance with the Conditions and Maintenance of Certification requirements
- The Cures Act, authorizes OIG to investigate claims that a health IT developer of certified health IT has engaged in information blocking

    - ONC and OIG are actively coordinating on establishing referral policies and procedures to ensure the timely and appropriate flow of information related to information blocking complaints
    - Enforcement of information blocking civil monetary penalties (CMPs) will not begin until established by future notice and comment rulemaking by OIG
- The Act also requires ONC to implement a standardized process for the public to submit reports on claims of health information blocking – ONC is working to build off of existing processes