AUDACIOUS INQUIRY | BOLD SOLUTIONS FOR CONNECTED HEALTHCARE

ONC Cures Act Final Rule Summary

ONC's Cures Act Final Rule fosters innovation in healthcare to advance patients' control of their health records, promotes a modern app economy, and defines exceptions to information blocking.

On March 9th, 2020, ONC released its Cures Act Final Rule and it was published in the Federal Register May 1, 2020. The Final Rule implements key provisions outlined in the 21st Century Cures Act to advance interoperability, support seamless exchange, access, and use of electronic health information, and addresses information blocking.

Enforcement Discretion Due to COVID-19

Due to the COVID-19 pandemic, ONC announced that it will be exercising enforcement discretion for many of the new certification related requirements in the Final Rule. ONC revised its compliance dates and timeframes to three (3) months after each initial compliance date or timeline identified in the Final Rule. The revised timeframes for compliance are reflected in this summary document.

Changes to Information Blocking

The Cures Act defined and prohibited information blocking generally by covered actors, which are health IT developers of certified products, healthcare providers, health information exchanges (HIEs), and health information networks (HINs). In the Final Rule, ONC defines key terms to clarify the Cures Act definition of information blocking, provides examples of conduct that would constitute information blocking, and outlines eight detailed exceptions of practices that would not constitute information blocking. The eight exceptions fall into two categories: 1) exceptions that involve *not fulfilling requests* to access, exchange, or use electronic health information (EHI) and 2) exceptions that involve *procedures for fulfilling requests* to access, exchange, or use EHI. ONC notes repeatedly in the Final Rule that if an actor's practice does not meet the conditions of an exception, it will not automatically constitute information blocking. Such practices will be evaluated on a case-by-case basis to determine if information blocking has occurred.

The eight exceptions to information blocking are:

- Exceptions that involve *not fulfilling requests* to access, exchange, or use EHI: It is not considered information blocking if…
    1. Preventing harm exception: an actor engages in practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met.
    2. Privacy exception: an actor does not fulfill a request in order to protect an individual's privacy, provided certain conditions are met.
    3. Security exception: an actor interferes with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met.
    4. Infeasibility exception: an actor does not fulfill a request due to the infeasibility of the request, provided certain conditions are met.

5. Health IT performance exception: an actor takes reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met.

- Exceptions that involve *procedures for fulfilling requests* to access, exchange, or use EHI: It is not considered information blocking if…
    6. Content and manner exception: an actor limits the content of its response to a request to access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI, provided certain conditions are met.
    7. Fees exception: an actor charges fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI, provided certain conditions are met.
    8. Licensing exception: an actor licenses interoperability elements for EHI to be accessed, exchanged, or used, provided certain conditions are met.

Covered actors must comply with the information blocking requirement nine months after the publication of the Final Rule; however, enforcement will not begin until future rulemaking is finalized. The Cures Act gives the HHS Office of the Inspector General (OIG) authority to investigate claims of information blocking. Health IT developers, HIEs, and HINs found to be information blocking can face civil monetary penalties (CMP) of up to $1 million per incident. In the rule, ONC notes that enforcement of information blocking for health IT developers of certified products and HIEs/HINs will not start until the OIG establishes the CMPs through future rulemaking. ONC notes that discretion will be exercised such that conduct that occurs before OIG finalizes the rule will not be subject to the information blocking CMPs. Healthcare providers found to be information blocking will be referred to relevant agencies (i.e. CMS) and face applicable disincentives that generally will be adopted through future rulemaking. Today, the only applicable disincentive for a provider found to be information blocking is that they would fail the Medicare or Medicaid Promoting Interoperability Program or the Merit-based Incentive Payment System (MIPS) Promoting Interoperability performance category.

ONC modified the definition of EHI to align it with ePHI that would be included in a designated record set. For the next 24 months, covered actors only need to exchange data elements in the United States Core Data for Interoperability (USCDI) instead of the full EHI to be in compliance. After two years, the scope of information blocking includes the full EHI definition.

Any health IT developer that has a product certified through the ONC Health IT Certification Program is prohibited from information blocking and can face fines and/or the loss of their certification. This prohibition applies to all products offered by a health IT developer that has a certified product, not just to their certified products.

Changes to the Health IT Certification Program

The Cures Act Final Rule makes several changes to ONC's Health IT Certification Program (Program), including adding new criteria, revising existing certification criteria, establishing initial requirements that

health IT developers and their modules must meet to get certified, and defining ongoing requirements that must be met by the developer and their modules to maintain certification. For example:

- Information Blocking: Health IT developers are prohibited from information blocking and could face removal from the Program if they are found to be information blocking.
- Communications: Developers are not allowed to prohibit or restrict communications regarding the following subjects:1) Usability; 2) Interoperability; 3) Security; 4) User experiences; 5) Developer business practices related to the exchange of EHI; 6) The manner in which a user of the health information technology has used such technology. ONC allows for certain exceptions to the requirements.
- Real World Testing: Requires that health IT developers successfully test the real-world use of the technology for interoperability in the type of setting in which such technology would be marketed.

United States Core Data for Interoperability (USCDI)

The ONC Cures Act Final Rule adopts the first version of the USCDI as a standard that ultimately replaces the Common Clinical Data Set (CCDS). The USCDI establishes a minimum set of data classes that are required to be interoperable nationwide and are designed to be expanded in an iterative and predictable way over time. Health IT developers will be able to take advantage of the new Standards Version Advancement Process (SVAP) and voluntarily update certified products to newer National Coordinator approved versions of the USCDI without waiting for rulemaking.

The USCDI is comprised of data classes and data elements (i.e., “patient demographics” is a data class and within that data class is “patient name”, which is a data element). Adoption of the USCDI will advance interoperability by ensuring utilization of common data and vocabulary codes sets. This standardization will support both electronic exchange and usability of the data.

The USCDI version 1 adds three new data classes (Clinical Notes, Provenance, Allergies and Intolerances), and additional data elements to Patient Demographics and Pediatric Vital Signs. The list below identifies the new items that ONC has included in the USCDI compared to the CCDS:

- Clinical Notes (New)
  - Discharge Summary Note
  - History & Physical
  - Progress Note
  - Consultation Note
  - Imaging Narrative
  - Laboratory Report Narrative
  - Pathology Report Narrative
  - Procedures Note
- Provenance (New)
  - Author time stamp
  - Author organization

- Allergies and Intolerances (New)
  - Substance (Drug Class)
  - Reaction
- Patient Demographics (Expanded)
  - Current Address
  - Previous Address
  - Phone Number
  - Phone Number Type
  - Email Address
- Vital Signs (Expanded to include pediatrics)
  - Head Occipital-frontal circumference percentile (Birth to 36 Months)
  - Weight-for-length percentile (Birth to 36 Months)
  - BMI percentile (2-20 Years of Age)

ONC will establish and follow a predictable, transparent, and collaborative process to expand the USCDI overtime, which will provide stakeholders with the opportunity to comment on the USCDI's expansion and to advance additional data classes and data elements relevant to a wide range of use cases related to healthcare.

Standards Version Advancement Process (SVAP)

ONC established the voluntary Standards Version Advancement Process (SVAP) to enable health IT developers' to update certified products to more advanced versions of standards and implementation specifications that have been approved by the National Coordinator. The SVAP enables the advancement of standards without being constrained to rulemaking. Health IT developers are required to provide advance notice to their clients and ONC-Authorized Certification Body (ONC-ACB) before adopting new standards and must undergo real world testing.

Electronic Health Information (EHI) Export

ONC finalized the new EHI export criterion § 170.315(b)(10), which requires a certified health IT module to electronically export all of the EHI, as defined in § 171.102, that can be stored at the time of certification by the product, of which the health IT module is a part. This includes exporting EHI to support single patient EHI access requests as well as support for healthcare providers interested in exporting an entire patient population to transition to another health IT system. Certified health IT developers must roll out EHI export capabilities and provide the technical capabilities expressed in § 170.315(b)(10) no later than 39 months after the publication of the Final Rule.

- Single Patient EHI Export ((§170.315(b)(10)(i)): The single patient export functionality includes the capability for a user to execute a single patient export and must be able to be limited at least one of two ways: (1) to a specific set of identified users, and (2) as a system administrative function. A user must be able to execute the single patient EHI export capability at any time the user chooses and without subsequent developer assistance to operate regardless of whether the developer is

operating the export for a healthcare provider or a healthcare provider is maintaining and operating the technology in their own production environment.

- Patient Population EHI Export ((§170.315(b)(10)(ii)): The patient population EHI export functionality supports patient data transitions in instances of healthcare providers switching health IT systems. Certified health IT developers are required to provide reasonable cooperation and assistance to other persons, such as customers, users, and third-party developers, to ensure the capability is deployed in a way that enables the successful migration of patient data.
- Standard/Format: The certification criterion does not require a specific standard format to be used. The export files, for both the single patient and the patient population EHI export functionalities, must be electronic, in a computable format, and include the publicly accessible, up-to-date hyperlink of the export's format, which allows any person to directly access the information without any preconditions or additional steps.
- Stored Data: "Stored" data applies to all EHI and is agnostic as to whether the EHI is stored in or by the certified health IT module or in or by any of the other "non-certified" capabilities of the health IT product of which the certified health IT module is a part.
- Image Data: For conformance, any images, imaging information, and image elements that fall within the scope of EHI for this certification criterion will need to be exported unless links to images/imaging data (and not the images themselves, which may remain in a PACS) are the only EHI stored in or by the product to which this certification criterion applies in which case only the links would need to be part of the export.
- Timeframe: Neither type of export will require the Health IT Module to support a specific or user-defined timeframe range or time limit in order to demonstrate conformance.
- "Direct-to-patient" Functionality: This certification criterion does not require "direct-to-patient" functionality in order to demonstrate conformance.

Standardized Application Program Interfaces (API) for Patient and Population Services

The ONC Cures Act Final Rule establishes new application program interfaces (API) requirements for health IT developers. Starting 27 months following publication of the Final Rule, the new API certification criterion, § 170.315(g)(10), will replace the "application access—data category request" certification criterion (§ 170.315(g)(8)). This new criterion requires standardized API access for single patient and population services and is limited to API-enabled "read" only services using the Health Level 7 (HL7®) Fast Healthcare Interoperability Resources (FHIR®) standard.

ONC has outlined the following requirements for certified health IT developers and their certified API technologies to meet:

- Base Standard: ONC is requiring the use of HL7®FHIR® Standard Release 4.0.1.
- Data Access and Search: For both single and population services, the API technology is required to respond to requests for data specified in the USCDI version 1 according to the US FHIR Core implementation Guide (US FHIR Core IG) for FHIR Release 4. For multiple patients' data, the API technology must support "group-level export" according to the Bulk Data Access Implementation

Guide. Additionally, the API technology will need to support all required search criteria specified in US FHIR Core IG for access requests with patient and user scope.

- Software Application (App) Registration: Apps will need to be registered with the API technology's "authorization server" prior to interacting with the API technology.
- Publicly Accessible Technical Documentation: The certified API technology must make all technical documentation necessary for developers to design and register apps that interact with the API available via a publicly accessible hyperlink.
- Security: ONC requires the API technology to establish a secure and trusted connection with apps using Transport Layer Security (TLS) version of 1.2 or higher for all transmissions. The API technology must perform additional authentication and authorization using specified implementation specifications before providers can use the app for clinical purposes or before an app is authorized for a patient to receive their data. These include:
    - Apps connecting with the API technology must support authentication and authorization according to SMART app Launch Implementation Guide (including "patient" and "user" scopes) and the OpenID Connect standard.
    - The API technology must issue a refresh token for at least three months to apps capable of maintaining a "client secret".
    - When requesting access to multiple patients' data using "system scopes," the API technology must perform authentication and authorization during the process of granting an app access to patient data in accordance with the "SMART Backend Services Authorization Guide" section of the Bulk Data Access Implementation Guide.
- Patient Authorization Revocation: When directed by a patient, the API technology's authorization server must be able to revoke an authorized app's access to that patient's data.
- Token Introspection: The API technology's authorization server must provide capability to receive and validate tokens it has issued.
- Permitted Fees: ONC outlines the permitted fees that can be charged. Generally, any fees not outlined are prohibited.
    - Health IT developers that have certified API technology are permitted to charge fees to healthcare organizations that deploy the API for the development, deployment, and upgrade of their certified API technology, and towards recovering API usage costs (if applicable).
    - Health IT developers that have certified API technology are also permitted to charge app developers for value-added services related to certified API technology, so long as such services are not necessary to efficiently and effectively develop and deploy production-ready software that interacts with certified API technology.
- Openness and pro-competitiveness: ONC establishes practices that health IT developers with certified API technology must follow to enable an open and competitive marketplace. For example, ONC generally requires certified API developers to grant healthcare organizations that deploy the API the independent ability to permit apps to interact with the certified API deployed by the healthcare organization.

- Health IT developers that have certified API technology are permitted to charge fees to healthcare organizations that deploy the API for the development, deployment, and upgrade of their certified API technology, and towards recovering API usage costs (if applicable).
- Health IT developers that have certified API technology are also permitted to charge app developers for value-added services related to certified API technology, so long as such services are not necessary to efficiently and effectively develop and deploy production-ready software that interacts with certified API technology.

About Audacious Inquiry and our Consultants

Audacious Inquiry (Ai) is a health information technology (Health IT) and policy company that is making healthcare more connected. We facilitate the exchange of health information to deliver care coordination solutions. Our software is designed to be efficient and cost-effective, our nationally-recognized team-members provide tactful strategic consulting, and our services rethink how health information is shared, managed, leveraged, and protected.

Our Strategic Advisory practice offers consulting services to government entities, HIOs, providers, and payers/ACOs in the areas of:

- Health IT Policy
  Market research and evaluation, legislative and regulatory analysis, and guidance for industry compliance
- Road-mapping & Advisory
  Health IT evaluation and guidance to support long-term objectives and Delivery System Reform
- Medicaid Technology & Operations
  Planning and funding strategy, contracting strategy, re-use and modularity plans
- Outreach & Onboarding
  Methods for rapid adoption of health information exchange
- Creative Communications
  Visual communication tactics to support marketing and branding efforts

Further questions?

- Please contact Kory Mertz at: kmertz@ainq.com.