Key Takeaways of CMS and ONC Interoperability Rules

Updated as of July 8, 2020

I. Background

On March 9 the Office of the National Coordinator for Health IT (ONC) and the Centers for Medicare & Medicaid Services (CMS) published their companion interoperability rules. These execute and deliver on requirements contained in the 21st Century Cures Act, as well as Executive Order 13813 aimed at competition and choice.

On May 1, both the ONC and CMS rules were finalized in the Federal Register. Changes within the final rules included delays to multiple timelines, including a twelve-month delay to the CMS admission, discharge and transfer (ADT) notification requirements and a three-month delay to ONC's information blocking compliance and enforcement timelines.

II. ONC Rule

A. *Links*

- **Rule**
- **High-level timelines document**
- **Website** on the new rule
- **Press Release**
- **Difference between proposed rule and final rule**
- **Enforcement Discretions**
- **Blog post**
- **USCDI**
- **Information Blocking Exceptions Companion Guide**

B. *Electronic health information (EHI)*

- **Compliance deadline:** Six months following publication of final rule (November 2, 2020).
- More narrow definition adopted than proposed.
- **6-24 months** (lasting thru May 1, 2022) following publication of the final rule EHI is defined as data elements in the U.S. Core Data for Interoperability (USCDI). Following **24 months** (starting May 2, 2022), the definition changes to electronic protected health information (ePHI).

C. *Updates to 2015 CEHRT*

- **Compliance Deadlines:** Vendors have **24 months** (May 2, 2022) from the time the rule is finalized until when all changes with the exception of EHI export must be made; they have **36 months** (May 2, 2023) for EHI export.

- **General:**
  - ONC is not putting out a new edition, however, they will distinguish it between the existing 2015 CEHRT with the new name, *2015 Edition Cures Update.*

- **EHI Export:**
  - ONC requires certified products be able to support use cases without developer assistance in real time.
  - Two use cases include: EHI Export for patient-initiated requests; and patient population EHI export.
  - No standard format is required for export; however, it must be made available via a publicly available hyperlink.
  - **NOTE:** Providers must be capable of exporting EHI even if it is not in a certified product. ONC states, "a health IT user may have other health IT systems with no connection to the Certification Program that store EHI and such EHI would still be in scope from an information blocking perspective."

- **Application programming interfaces (APIs)**
  - **Compliance deadline:** Within **24 months** (May 2, 2022) of publication of final rule
  - FHIR Release 4 was adopted.
  - **Privacy and Security of APIs**
    - **ONC writes,** ""Vetting" in the example's context meant a determination regarding whether the app posed a security risk to the EHR developer's API, which may be the situation with a proprietary API. For certified API technology, which includes the use of OAuth2 among other security requirements in addition to its focus on "read-only"/responses to requests for EHI to be transmitted, 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). Thus, for third-party applications chosen by 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."
    - However, they also note, "That actors, such as health care providers, have the ability to conduct whatever 'vetting' they deem necessary of entities (e.g., app developers) that would be their business associates under HIPAA before granting access and use of EHI to the entities. In this regard, covered entities must conduct necessary vetting in order to comply with the HIPAA Security Rule."

- On providers' concerns about third-party apps selling patient information, ONC says, "This final rule supports an individual's ability to choose which third party developer and app are best for receiving all or part of their EHI from a health care provider and to agree to clear and public terms of use on how that initial and ongoing engagement with the third-party developer and app occurs."
- ONC also says they support and strongly encourage providing individuals with information that will assist them in making the best choice for themselves in selecting a third-party application.
- ONC declined to go so far as to require API technology suppliers to verify that an app has a privacy notice. Instead, they call on "actors" (those required to meet information blocking) to, "educate patients and individuals about the risks of providing other entities or parties access to their EHI." They furthermore state, "This type of education can be designed to inform the patient about the privacy and security practices of the third party and the third-party app, including whether the third-party developer has not acted in accordance with elements of its privacy policy."
- ONC offers a set of minimum best practices to be followed by third parties (voluntary not mandatory).

- **Information Blocking:**
  - **Actors:** Per the Cures Act, information blocking only applies to four sets of actors:
    - **Providers:** ONC maintained an expansive definition of types of providers. Providers that own health information exchanges (HIEs) or health information networks (HINs) are not considered HIEs/HINs (subject to higher fines for blocking per the law) when acting in their role as a provider.
    - **Vendors:** Includes individuals and entities that develop or offer certified health IT. Providers that develop their own EHR and get it certified are not included.
    - **HIEs and HINs:** ONC combined the two categories into one. Excludes social networks, internet service providers and technology that facilitates exchange of information.
  - **Penalties:** The 21st Century Cures Act set forth penalties up to $1 million per violation for instances of information blocking for all actors except providers. Provider penalties will be announced in forthcoming rules.
  - **Exceptions:** An actor found to have met one of the eight exceptions outlined by ONC will not be subject to information blocking penalties. The eight exceptions include:

- Preventing Harm
- Privacy
- Security
- Infeasibility
- Health IT Performance
- Content and Manner
- Fees
- Licensing

- **Compliance date: 6 months** (November 2, 2020) following publication of the final rule.

- **Enforcement:**
  - Future rulemaking will be needed to outline information blocking disincentives for providers that do not comply with the information blocking requirements.
  - ONC previously stated it's possible that enforcement for providers could be retrospective to November 2, 2020, and thus providers should be prepared for compliance by that date.
  - Enforcement for vendors, health information networks (HINs), and health information exchanges (HIEs) – as outlined in the Office of the Inspector General (OIG) civil monetary penalties proposed rule. released on April 24, 2020 – will either be 60 days from publication of the final rule or another alternative date.

III. CMS Rule

A. Links

- **Rule**
- **High-level timelines document**
- **Website** on the new rule
- **Fact Sheet**

B. Admission, Discharge and Transfer:

- **Updated: Compliance deadline: 12 months** (May 1, 2021) following publication of final rule.
- CMS finalized a slightly modified version of its proposal.
- Hospitals, psychiatric hospitals and critical access hospitals (CAHs) will be required to send electronic notices of admission, discharge, or transfer (ADT) to certain providers where they have certified EHR systems capable of sending such notices.
- The final rule narrows the group of providers to whom patient event notifications must be sent.
- Allows hospitals to exercise reasonable effort to send patient event notifications.

- Declines to specify a standard that must be used for patient event notifications.
- Determines the circumstances under which a patient event notification is to be sent.
- Clarifies the implications of this rule on patient privacy, noting the rule may conflict with other federal or state laws. For instance, under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, patients have the ability to limit the disclosure of their health information to practitioners of their choosing.
- ADT notices are to be sent upon patient's:
    - Registration in the hospital's emergency department (ED).
    - Admission to the hospital's inpatient services.
    - Discharge or transfer from the hospital's ED.
    - Discharge or transfer from the hospital's inpatient services.
- The final rule requires hospitals to use "reasonable effort to ensure" that the specified providers are notified of the patient's status.