Executive Summary of Final Rule

Background

The landmark *21st Century Cures Act* was signed into law in December 2016. Many of the provisions in the law focused on improving interoperability of health information.

Last week, on March 9, the Centers for Medicare & Medicaid Services (CMS) issued regulations implementing these provisions, largely focused on patient access to health information. Coupled with the ONC Final Rule, released on the same day by the Office of the National Coordinator for Health IT (ONC), the CMS Final Rule takes unprecedented steps to advance health information interoperability.

Key Takeaways from the Final Rule

- CMS notes frustration with siloed patient information and believes patients should be able to move between payers and providers and take their health information with them

- CMS believes payers are uniquely situated to provide enrollees with comprehensive information on their claims and encounter data
  - In order to achieve this, CMS is requiring Medicare Advantage organizations, Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and Qualified Health Plan (QHP) issuers on Federally Facilitated Exchanges (FFEs) to implement and maintain a standards-based Patient Access API, which must meet technical standards finalized in the ONC Final Rule

- Payers must allow third-party applications to retrieve, with the approval and at the direction of the current enrollee, certain data:
  - Adjudicated claims
  - Encounters with capitated providers
  - Clinical data, including laboratory results (when maintained by the payer)

- In response to many commenters who raised concerns about privacy and security of data once sent to third-party applications, CMS largely points to current laws – HIPAA and the Federal Trade Commission Act, noting that it does not have the authority to regulate third-party applications

- CMS places responsibility on health plans to educate enrollees about the risks associated with sending their health information to third-party apps that are not subject to HIPAA via Business Associate Agreements. Plans are required to post

privacy- and security-related resources to their websites, for which CMS will provide suggested content, and such resources should include a discussion about a third-party app's secondary use of data

- The statute allows HHS to establish "appropriate disincentives" for providers who information block. CMS has decided to implement this by publicly naming – through an indicator on Physician Compare – an eligible clinician or group who submits a "no" response for any of the three prevention of information blocking statement for MIPS
    - Important to note that this only applies to MIPS eligible clinicians or groups

- Like the ONC Final Rule, the implementation deadlines in the CMS Final Rule are staggered
    - Hospitals must send event notifications 6 months after publication of the Final Rule
    - In late 2020, required public reporting of hospitals and/or clinicians who attest to information blocking and providers without digital contact information
    - By January 1, 2021, payers must implement the Patient Access API and the Provider Directory API
    - By January 1, 2022, payers are required to exchange patient data upon request
    - States must send buy-in data daily by April 2022

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

Detailed Summary of Final Rule

Overview of Major Provisions

Patient Access and Provider Directory APIs

- Requires MA organizations, Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and QHP issuers on FFEs to implement and maintain a standards-based Patient Access API
    - The API must meet technical standards finalized in the ONC Final Rule
- Payers must permit third-party applications to retrieve, with the approval and at the direction of the current enrollee, certain data:
    - Adjudicated claims – including provider remittances and enrollee cost-sharing
    - Encounters with capitated providers
    - Clinical data, including laboratory results (when maintained by the payer)
- Data must be made available no later than one business day after a claim is adjudicated or encounter data are received
- Beginning January 2021, payers have to make available through the Patient Access API the specified data they maintain with a date of service on or after January 1, 2016
- Requires MA organizations, Medicaid and CHIP FFS programs, Medicaid managed care plans, CHIP managed care entities, and QHP issuers on FFEs to make standardized information available about their provider network through a Provider Directory API that is consistent with technical standards, except the security protocols related to user authentication and authorization or any other protocols that restrict availability of this information
    - Security protocols are not necessary when making publicly available data accessible via an API
- Payers must make available (at a minimum) – provider names, addresses, phone numbers, and specialties
- For MA organizations that offer MA-PD plans, they must make available (at a minimum) – pharmacy directory data, including the pharmacy name, address, phone number, number of pharmacies in the network, and mix (specifically the type of pharmacy, such as "retail pharmacy")
- All directory information must be made available to current and prospective enrollees and the public through the Provider Directory API within 30 calendar days of a payer receiving provider directory information or an update to the provider directory information
- The Provider Directory API must be fully implemented by January 1, 2021
- Requires MA organizations, Medicaid managed care plans, CHIP managed care entities, and QHP issuers on the FFEs to coordinate care between payers by exchanging, at a minimum, the data elements specified in the current content and vocabulary standard finalized by ONC – USCDI version 1

- Payer must send, at a current or former enrollee's request, specific information they maintain with a date of service on or after January 1, 2016 to any other payer identified by the current or former enrollee
- Payer is only obligated to share data received from another payer under this regulation in the electronic form and format it was received

Trusted Exchange Networks

- CMS is not finalizing their proposal for MA organizations, Medicaid managed care plans, CHIP managed care entities, and QHP issuers on the FFEs to participate in a trusted exchange given the concerns commenters raised regarding the need for a mature Trusted Exchange Framework and Common Agreement (TEFCA) to be in place first

Coordination of Dually Eligible Individuals

- Requires all states participate in daily exchange of buy-in data, which includes both sending data to CMS and receiving responses from CMS daily, and that all states submit the MMS file data to CMS daily by April 1, 2022
    - This will improve the experience of dually eligible individuals

Privacy and Security Concerns

- Deploying API technology would not lessen any such covered entity's duties under HIPAA and other laws to protect the privacy and security of information it creates, receives, maintains, or transmits, including but not limited to PHI
- A CE implementing an API to eligible individuals to access their health information must take reasonable steps to ensure an individual's information is only disclosed as permitted or required by applicable law
- The entity must take greater care in configuring and maintaining the security functionalities of the API and the CEs' electronic information systems to which it connects than would be needed if it was implementing an API simply to allow easier access to widely available public information
- If an individual requests their PHI in an EHR be sent to the third party by unencrypted email or another unsecure manner, which the individual has a right to request, reasonable safeguards could include, for example, carefully checking the individual's email address for accuracy and warning the individual of risks associated with the unsecure transmission
- HIPAA CEs and Bas continue to be responsible for compliance with the HIPAA Rules, the Federal Trade Commission Act, and all other laws applicable to their business activities, including but not limited to their handling of enrollees' PHI and other data

- CMS pointed to OCR guidance that notes that CEs are not responsible under the HIPAA Rules for the security of PHI once it has been received by a third-party application chosen by an individual
- When a non-covered entity discloses an individual's confidential information in a manner or for a purpose not consistent with the privacy notice and terms of use to which the individual agreed, the FTC has authority under section 5 of the FTC Act to investigate and take action against unfair or deceptive trade practices
- The FTC also enforces the FTC Health Breach Notification Rule, which applies to certain types of entities, including vendors of personal health records and third-party service providers, that fall outside of the scope of HIPAA and therefore, are not subject to the HIPAA Breach Notification Rule
- CMS is requiring Enrollee and Beneficiary Resources Regarding Privacy and Security
- There are some cases when data would be required to be made available under the HIPAA patient access requirement, but not required to be transferred through the API – for instance, when the CE does not hold certain information electronically
- CMS notes recent court decision in Ciox Health, LLC v. Azar, et al, which vacates a portion of the HIPAA Privacy Rule that provides an individual the right to direct a covered entity to send protected health information that is not in an EHR to a third party identified by the individual
- The only instance per the policies in the rule that would allow a payer to deny access to an app would be if the CE or BA's own systems would be endangered if it were to engage with a specific third-party application through an API – for instance if allowing such access would result in an unacceptable security risk
- CE and BA efforts must stop at education and awareness or advice regarding concerns related to a specific app
    - For instance, if a payer notes that an app a patient requests receive their data does not lay out in its privacy policy specifically how the patient's personal data will be used, the payer could choose to inform the patient they may not want to share their data with the app without a clear understanding of how the app may use the data, including details about the app's secondary data use policy
- CMS is sharing best practices and links to model language of an easy-to-understand, non-technical, consumer-friendly privacy policy, building off of lessons learned with Blue Button 2.0, to support payers and developers in this effort
- CMS also outlines a framework payers can use to request that third-party apps attest to covering certain criteria in their privacy policy, such as information about secondary data use

Enforcement

- Requires inclusion of an indicator on Physician Compare for the eligible clinicians and groups that submit a "no" response to any of the three prevention of information blocking statements for MIPS

    - In the event the statements are left blank, attestations will be considered incomplete, and CMS will not include an indicator on Physician Compare
    - The indicator will be posted on Physician Compare, either on the profile pages or in the downloadable database, starting with the 2019 performance period data available for public reporting starting in late 2020
    - Would only apply to Merit-Based Incentive Payment System (MIPS)-eligible clinicians or groups
- Including information on a publicly available CMS website indicating that an eligible hospital or critical access hospital (CAH) attesting under the Medicare FFS Promoting Interoperability Program has submitted a "no" response to any of the three attestation statements related to the prevention of information blocking
    - In the case that there is a "blank" response, the attestations will be considered incomplete, and no information will be posted related to those attestation periods
    - CMS will post information starting with the attestations for the EHR reporting period in 2019 and expect this information will be posted in late 2020
- CMS will publicly report the names and National Provider Identifiers (NPIs) of those providers who do not have digital contact information included in the National Plan and Provider Enumeration System (NPPES) beginning in the second half of 2020
- Requires a hospital, psychiatric hospital, and CAH, which utilizes an electronic medical records system or other electronic administrative system that is conformant with the content exchange standard (USCDI) to demonstrate that:
    - Its system's notification capacity is fully operational and that it operates in accordance with all state and federal statutes and regulations regarding the exchange of patient health information;
    - Its system sends notifications that must include the minimum patient health information specified – patient name, treating practitioner name, sending institution name, and if not prohibited by other applicable law, patient diagnosis
    - Its system sends notifications directly, or through an intermediary that facilitates exchange of health information, and at the time of a patient's registration in the emergency department or admission to inpatient services, and also prior to, or at the time of, a patient's discharge and/or transfer from the emergency department or inpatient services, to all applicable post-acute care services providers and suppliers, primary care practitioners and groups, and other practitioners and groups identified by the patient as primarily responsible for his or her care, and who or which need to receive notification of the patient's status for treatment, care coordination, or quality improvement purposes
    - Will be applicable 6 months after publication of this rule for hospitals, including psychiatric hospitals, and CAHs