Crowell

CLIENT ALERT

CMS Proposes New Requirements on Health Plans to Release Data

February 11, 2019

Drawing on the vision set out in the 21st Century Cures Act, CMS has issued a new proposed regulation that would require all health plans subject to CMS authority to make certain clinical, claims, and coverage information available to patients and their personal representatives. Comments are due 60 days following publication in the Federal Register.

This regulation contains policy consistent with and linked to ONC's new proposed regulation implementing 21st Century Cures provisions, also released today. Together, both regulations propose sweeping and potentially transformative changes to the way data is accessed and exchanged in health care.

Where do these requirements come from?

The 21st Century Cures Act, a bipartisan bill passed in December 2016, contained several new requirements and programs intended to enhance the interoperable exchange of health information between stakeholders, including patients, providers, electronic health record (EHR) vendors, health information exchanges, networks, and more. Among other provisions, the legislation urged the implementation of application programming interfaces (APIs) to modernize data exchange and better facilitate patient access to their own health information.

The Trump Administration has doubled down on previous efforts to improve interoperable patient access to health information, including Executive Order 13813 to Promote Healthcare Choice and Competition Across the United States, and a multi-agency initiative called MyHealtheData.

Who is impacted?

With a few exceptions, CMS is proposing these new requirements for Medicare Advantage organizations, Medicaid managed care plans, Medicaid state agencies, CHIP managed care entities, CHIP agencies operating fee-for-service (FFS) systems, and qualified health plans (QHPs) in the federal exchanges.

What will entities need to do to comply?

These plans and agencies will need to make certain information accessible to patients through an open API, consistent with their existing obligations under the HIPAA Privacy Rule. The requirements below are generally consistent across entity types, with some exceptions or slight variations.

- *Patient Access to Data*:
    - Claims and Encounters: Adjudicated claims (approved or denied), encounters with capitated providers, provider remittances, enrollee cost-sharing, and all clinical data including laboratory results.

- ○ Provider Directories: Plans' networks of contracted providers, including providers' names, addresses, phone numbers, and specialties.
- ○ Pharmacy Directories: MA organizations offering Part D plans must also offer the number, mix, and addresses of pharmacies in their network.
- ○ Formularies: Information about covered outpatient drugs and preferred drug lists.
- ○ Administrative: Enrollee identifiers, dates of service, and payment information should be included.

- *Timeliness*: In general, with some exceptions, the timeline on all impacted entities for making this data available to the patient is one business day upon claim processing or data receipt. For provider directory data, the proposal states that plans would be required to update the information available no later than 30 calendar days after changes are made or the entity receives updated information.
- *Open API*: CMS is defining an "open API" as one for which the documentation and guidance is openly published, such that any third-party developer could easily access the technical, financial, business, legal, or other information needed to connect to the API. CMS offers three policy goals for API attributes: (1) that the APIs are standardized, (2) that they are technically transparent, and (3) that they are implemented in a pro-competitive manner. To the first point, CMS is primarily linking its proposed requirements to the Fast Healthcare Interoperable Resources (FHIR), OAuth and OpenID Connect Core standards, consistent with ONC's new proposed certification criteria for APIs, although the agency will provide leeway for data types that do not neatly fit in an existing FHIR resource, or where another standard is more appropriate, such as the HIPAA Administrative Simplification transaction standards. Any documentation associated with the API must be publicly accessible on the entity's website or another public URL – for example, it cannot be behind a paywall or only available via email.

What about privacy and security?

Many covered entities, both providers and plans, have raised concerns about privacy and security that may result when allowing third-party applications to pull the data they hold. Many direct-to-consumer applications are not covered under HIPAA, and are only held to the provisions they create and make transparent in their privacy policies and other documentation. The Federal Trade Commission has the authority to enforce against unfair and deceptive practices – such as when a company violates its own privacy policy – but does not set rules and restrictions about what these applications must do with consumer data.

Under CMS's proposal, plans can place limits on applications that pose an untenable security risk to their systems, consistent with their own security risk assessment and obligations to protect PHI under HIPAA. In CMS's words, "a covered entity is not expected to tolerate unacceptable levels of risk to the PHI held by the covered entity in its systems." Entities would still be able to deny or terminate some applications from their API program if the entity determines that the level of risk is unacceptable, or if an application violates the terms of service or other contractual agreement. This determination must be based on "objective, verifiable criteria" that is "applied fairly and consistently across all applications," to avoid discrimination against competitors or certain types of third party organizations.

However, CMS is clear that any plan's policies or procedures for API access should be necessary for security purposes and not anti-competitive. For example, entities may not ban third party organizations entirely, only specific applications (giving the third party a chance to remediate a security concern and re-apply for access). CMS suggests that some types of information, such as electronic provider directories, are not patient-specific and may pose less risk – and the agency expects that entities would take this consideration into account when conducting its security risk assessment.

CMS also reiterates that covered entities, including the entities impacted by this proposed regulation, are not responsible under HIPAA for the security of PHI once it has been received by a third-party application. Given that there is no other federal regulatory framework for these applications beyond the FTC's enforcement authority, CMS proposes placing some additional responsibility on entities impacted by this rule to educate patients about the relative risks. Entities would need to inform patients about the risks of sharing their PHI with third-party applications, provide guidance on important considerations for selecting these applications, and educate patients on how to submit a complaint to appropriate federal agencies if they believe an application has violated the law. Such guidance must be given to patients in "non-technical, consumer-friendly language" and entities are responsible for updating it as needed.

Additional considerations

Plans may have a tough time making this data available within one business day if they do not receive the data, timely and complete, from their partners and other stakeholders. CMS anticipates this concern, but places the burden on plans to consider updates to their contracts to include "timing requirements for submission of encounter data and claims." However, CMS also notes that much of this information (at least, the information routinely involved in claims processing) should already be electronically accessible via administrative transaction standards and other existing health IT standards, given that most claims are processed electronically today.

Other proposals and requests for information

The proposed regulation includes requirements modifying Conditions of Participation for hospitals and other types of providers to enable exchange of electronic patient event notifications for admission, discharge or transfer; implementing public API access to provider directory data; plan-to-plan exchange of information for care coordination; public reporting on information blocking attestation; and requiring plans to participate in trust networks to promote broader interoperability across the industry.

The proposed rule also contains Requests for Information about information sharing between payers and providers via APIs, patient matching, interoperability between dual-eligible populations, and advancing interoperability through new payment models.

Next steps

These proposed requirements will be finalized or modified in an upcoming regulation that CMS expects to release later in 2019. For MA organizations and QHP issuers, these requirements would go into effect on January 1, 2020. For Medicaid and CHIP organizations, the effective date is July 1, 2020. This does not provide much time for implementation since the rules will not be finalized until later this year.

Crowell & Moring's Digital Health team is here to help your organization understand and respond to these proposals.

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