Jun 16, 2025

Response to
CMS-0042-NC

From:

Smile Digital Health
US Office
2021 GUADALUPE STREET
SUITE 260
AUSTIN, TX 78705

TD–16. What are the tradeoffs of maintaining point-to-point models vs. shared network infrastructure?
a. Do current rules encourage scalable network participation?
b. What changes would improve alignment (for example, API unification, reciprocal access)?

Current rules do encourage scalable network participation, though our experience with payer customers grappling with the real-world challenges of reducing the burden of the prior authorization process on patients and providers we see additional opportunities for improvement.

Specifically, we must improve the identification of both providers and payers– leveraging the capabilities of the OpenID Connect (OIDC) identity protocol to better refine our understanding of the organizations involved in healthcare decision making and payment– while at the same time, further enhancing data protections. It would be helpful to have a better mechanism for reflecting the real-world hierarchy of organizations (where a provider is an employee / contractor of a healthcare provider organization, which in turn might be a department / subsidiary of a larger organization). Reflecting a hierarchy is just as important for payers (health insurance carrier s) who are organized by health plan, lines of business, etc.

A technical administrator for a provider organization could register and say their OIDC client represents <Business ID01> and the registration flow could then proceed to look up the officially published related IDs.
This way if a malicious party tried to claim to represent ID01 they would get stuck as they could not provide a client assertion signed with the private key that matches the officially published public key. Having this identification mechanism would more easily enable a “hub and spoke” trust pattern like a "join the network" type of contract– the equivalent of a Public Interface API but for legal agreements.

- As an Organization when I sign this "join the network" contract I agree to:
  - Provide APIs and data that follow rules x,y,z (e.g. CMS-0057 rule)
  - Grant access using National directory based registration
- When requesting data from other parties I will use the same API on their side and:
  - agree to treat the data in accordance with the rules established <here> (e.g. data consent / sharing called out in CMS-0057)
  - when I say the member gave me consent to request it means that the member really gave me consent and, when asked about that assertion, I can prove it