Comment to the CMS docket CMS-2025-0050

https://www.federalregister.gov/documents/2025/05/16/2025-08701/request-for-information-health-technology-ecosystem

The California Department of Technology (CDT) appreciates the opportunity to provide comments on CMS's ongoing efforts to enhance identity management and digital access within federal healthcare systems. Drawing from CDT's Digital Identity Framework, we strongly recommend that CMS prioritize privacy, user consent, and system interoperability in the design and implementation of any digital identity solution. In particular, CDT urges CMS to advance federated identity systems over centralized models, implement robust privacy and security protections, and ensure that any solution is grounded in public trust and inclusive by design.

CDT is responsible for the development, implementation, administration, and management of the California Digital ID Framework on behalf of California State agencies. The Framework is a collection of data, technology infrastructure, digital services, and governance that allows for secure, user-friendly use of digital identity management across California. It ensures that everyone is held to the same high standards, better protects privacy, and helps people easily access more of California's state programs and benefits by simplifying and streamlining eligibility verification across agencies.

The CDT digital identity program is partnering with state and federal entities - including CMS - to create a federated identity ecosystem. Using our expertise implementing solutions for California State agencies and using federal solutions like Login.gov and Blue Button 2.0 API, we provide the following comments.

1. Federated Identity Management: Empowering Choice and Minimizing Risk

CDT supports federated identity systems where multiple trusted entities can authenticate users without creating a single, centralized source of identity. Federated models have the following benefits:

- Reduces single points of failure: Decentralizing identity providers lowers the risk of systemic data breaches.
- Promotes user autonomy: Individuals can choose from multiple credentialing sources (e.g., state Medicaid systems, commercial IDPs, community-based organizations), fostering greater trust and accessibility.
- Supports interoperability: Federated systems allow different agencies and providers to interact securely while respecting user preferences and privacy.

- Avoids government overreach: Prevents CMS or HHS from becoming the sole arbiter of digital identity in the health space.

CMS Recommendation:
Adopt a standards-based federated identity architecture aligned with protocols such as OpenID Connect, and ensure participation from public and nonprofit identity providers—not just large private platforms.

2. Privacy Protection and Data Minimization

Healthcare identity verification inherently involves sensitive personal data. CDT urges CMS to implement a privacy-centric framework that includes:

- Data Minimization: Only collect data strictly necessary for verification. Avoid collecting unrelated attributes such as geolocation, financial history, or behavioral analytics
- Purpose Limitation: Clearly define and restrict how identity data can be used (e.g., only for access control or account recovery, not marketing or surveillance).
- User Transparency and Logging: Give individuals access to audit logs showing when and by whom their identity or data was accessed.
- Decentralized Storage Options: Encourage architecture that avoids massive central repositories of identity data, mitigating breach risks.

CMS Recommendation:
Require all participating identity providers to comply with NIST SP 800-63-3 privacy guidelines and ensure that any vendor relationships include enforceable data governance and accountability measures.

3. Equity and Accessibility

Digital identity systems must be inclusive by design. Many patients—especially Medicaid recipients, rural populations, and older adults—may not have smartphones, broadband access, or lack access to government-issued IDs like a drivers license.

CMS Recommendation:

- Ensure identity verification systems are multilingual, accessible, and compatible with assistive technologies.
- Maintain non-digital options and allow verification through community-based organizations or in-person services.
- Regularly assess systems for disparate impacts using equity audits and privacy threat modeling.

4. User Agency and Consent

CDT supports efforts to ensure patients remain in control of their digital identity and how it is used. Therefore we recommend CMS should ensure that identity use is always consent-based and revocable.

CMS Recommendation:

- Provide clear, plain-language notices on how digital identity data will be handled.
- Design for portability and interoperability, so users can seamlessly move between health systems without re-verifying identity multiple times.

CDT strongly supports CMS's efforts to improve digital access, but urges a deliberate, ethical, and federated approach to identity verification that protects privacy, enhances equity, and respects individual autonomy. We welcome continued engagement and are available for further dialogue as CMS advances this work.

Thank you for providing the opportunity to comment. If you have questions, please reach out to the CDT Digital Identity program.