June 16, 2025

SUBMITTED ELECTRONICALLY AT REGULATIONS.GOV

Centers for Medicare & Medicaid Services
Department of Health and Human Services
Attention: CMS-0042-NC
P.O. Box 8013
Baltimore, MD 21244-8013

Re: CMS-0042-NC Request for Information re Digital Health Products for Medicare Beneficiaries and the State of Data Interoperability and Broader Health Technology Infrastructure

To Whom it May Concern:

On behalf of Apple Inc. (Apple), we thank the Centers for Medicare & Medicaid Services (CMS) and the Assistant Secretary for Technology Policy (ASTP)/Office of the National Coordinator for Health Information Technology (ONC) for the opportunity to comment on the request for information (RFI) seeking input regarding the market of digital health products for Medicare beneficiaries as well as the state of data interoperability and broader health technology infrastructure (the RFI). At Apple, we believe individuals should be empowered with meaningful access to their health information. Our health and health and fitness features have been developed with two overarching principles: 1) They are all subject to rigorous scientific validation processes, in collaboration with medical community experts; 2) Our features put our users' privacy at the center and provide users with transparency and control, and the tools to protect their data.

I. APPLE IS AT THE FOREFRONT OF DIGITAL HEALTH ACCESS AND INNOVATION

A. Apple Health App & Health Records

The Health app is available on iPhone and iPad, and acts as a central and secure place for users to view all of their health information. Users can now store over 150 different types of health data from Apple Watch, iPhone, iPad, Vision Pro and connected third-party apps and devices, in addition to available health records data from connected institutions in the US, UK, and Canada. Our application programming interfaces (APIs) are enabling third-party developers to create new solutions that promote healthy lifestyles. There are now tens of thousands of apps on the App Store that use our HealthKit API, so they can incorporate data users choose to share for the Health app to offer innovative health and fitness experiences, with rigorous privacy and data protocols. Advanced sensors and built-in features in Apple devices such as Apple Watch give providers powerful insights into patient health and encourage patients to lead healthier lives. With data such as activity, heart health, mobility, sleep, and more, providers can get a more complete picture of patient health and can offer more personalized care. There are four privacy principles that inform everything we do at

Apple: data minimization, on-device processing, transparency and control, and security. We built each of these four pillars into our Health features from the beginning.

Additional information on how the Health app and HealthKit protect user privacy is available at this link: https://www.apple.com/privacy/docs/Health_Privacy_White_Paper_May_2023.pdf

Our features and technologies also contribute to paving the way for users to control their own health records. Within the Health app on iPhone and iPad users in the US, Canada, and the UK can download their medical records from multiple participating institutions and see them next to all of their other health information in the Health app. Health Records is now available to patients with an iPhone or iPad at over 9,000 institutions, across over 30,000 locations. Health Records uses FHIR (Fast Healthcare Interoperability Resources), a standard for transferring electronic medical records. In the US, the 21st Century Cures Act requires that institutions allow patients to electronically access their health records from their health institution and now requires they certify they use publicly available FHIR APIs. FHIR APIs are already incorporated into the Health app for the Health Records feature, so thousands more institutions will be eligible to be listed in the Health app and those using supporting EHR vendors can be added automatically over time.

We understand that many users appreciate having access to their health records from multiple providers in one place. Regarding FHIR APIs, we believe it's important to evaluate and test data quality and ensure accurate mapping of standardized terminologies. We see significant value in an industry-led, ticket-based system for reporting and tracking API issues that require resolution. Additionally, a centralized, up-to-date directory of these endpoints would enable users to connect with multiple providers where they've received care and download their health records more easily.

B. Mobile Drivers Licenses & IDs in Wallet

We are excited to see the RFI’s focus on strong digital identity solutions for verification and authentication across health care use cases. Apple has worked to support the issuance and use of standards-based digital identity credentials that enhance privacy. In recent years, US States, the federal government, industry groups, and standards organizations have been working increasingly to drive support for mobile driver’s licenses (mDL) as a way to prove identity. More than 15 jurisdictions are live or in deployment with standards-based mDL implementations. State-issued, standards-based implementations of mDLs can provide a valuable solution for identity use cases across the health care space.

Of note, to support and accelerate the work in the emerging mDL ecosystem, the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) has a program underway to build out reference implementations and best practices for mDL deployments. Health care comprises one of the initial key sets of use cases this program is focused on.

Since 2022, Apple has enabled driver’s licenses and state IDs to be added to Apple Wallet, which allows residents to seamlessly and securely add and present their IDs in person and in apps using iPhone or Apple Watch — and starting later this year, Verify with Wallet on the Web will offer users a way to seamlessly and securely share their ID in Apple Wallet with select websites for identity verification.   There is significant momentum among states to support standards-based mobile driver's licenses with 10 jurisdictions issuing IDs to Apple Wallet today and others planned or in deployment.

Standards-Based Approach

Apple has designed the ID in Apple Wallet using relevant ISO standards, which sets clear guidelines for the industry around protecting consumers’ privacy when presenting an ID or driver’s license through a mobile device. For in person interactions, the identity reader must adhere to ISO/IEC 18013-5.

For online use cases, Apple is supporting the W3C’s Digital Credentials API to enable websites to request identity document information from Apple Wallet and participant third party wallet apps installed on an iPhone. Apple follows the W3C Digital Credentials API-based transmission mechanism defined in Annex C of ISO/IEC 18013-7:2025, offering users significant user experience and security benefits when sharing their digital ID compared to alternative transmission mechanisms. The Webkit for Safari implementation of the W3C Digital Credentials API and Annex C of ISO/IEC 18013-7:2025 includes additional browser-level protections against phishing and relay attacks, and supports session persistence, enabling a seamless presentment flow without requiring users to switch between apps. Furthermore, adopting a standards-based approach ensures interoperability, allowing users to share their digital ID across any browser and digital wallet implementation that implements the same standard.

We recommend support for ISO/IEC 18013-5 for in person interactions and ISO/IEC 18013-7:2025 (Annex C) as a protocol over the W3C Digital Credentials API for online interactions to allow the presentation of mDLs and other mDOCs.

Privacy & Security

ID in Apple Wallet uses the privacy and security features that are built into Apple devices to help protect a user’s identity and personal information. Once an ID is added to Apple Wallet, the information is encrypted on a user’s device, so others — including Apple — cannot access it unless a user chooses to present it. Further, Apple and the state-issuing authority do not know when or to whom a user presents their driver’s license or state ID.   A user’s presentment history is encrypted and stored only on their device, and Apple cannot see or access this information.

Additional information on the Security of IDs in Apple Wallet is available at this link: https://support.apple.com/guide/security/security-of-ids-in-apple-wallet-secb569bf393/web

II. CONCLUSION

We support CMS and ASTP/ONC’s continued efforts to advance interoperability across the healthcare system. We believe this progress is essential to enabling a future in which users can access not only their clinical records but also schedule appointments and learn about their coverage and care options. We would be supportive of a world in which users can share patient generated data and self reported data like medications back to their providers to close the loop on their health care. As we push forward in this space, we remain committed to working with CMS and the broader community to ensure that interoperability efforts reflect a thoughtful balance: protecting user privacy while fostering an environment where developers can build innovative health solutions. Apple appreciates CMS and ASTP/ONC’s attention to our response to the RFI. We look forward to continued collaboration in building a health system that is more connected, user-focused, and responsive to individual needs.

Regards,

Tim Powderly
Senior Director, Government Affairs, Americas
Apple