June 16, 2025

The Honorable Mehmet Oz, MD
Administrator
Centers for Medicare & Medicaid Services
Department of Health and Human Services
P.O. Box 8013
Baltimore, MD 21244

Submitted electronically via www.regulations.gov

Re: Request for Information; Health Technology Ecosystem (CMS-0042-NC)

Dear Administrator Oz:

Kaiser Permanente appreciates the opportunity to comment on the Centers for Medicare & Medicaid Services (CMS) and the Assistant Secretary for Technology Policy (ASTP)/Office of the National Coordinator for Health Information Technology's (ONC) (collectively ASTP/ONC) request for information (RFI)[1] soliciting public comment to inform efforts to improve the health technology infrastructure.

Kaiser Permanente[2] is the largest private integrated health care delivery system in the United States, with more than 12.6 million members in eight states and the District of Columbia. Kaiser Permanente's mission is to provide high-quality, affordable health care services and to improve the health of our members and the communities we serve. In addition, Risant Health, a nonprofit organization created by Kaiser Foundation Hospitals, is dedicated to improving the health of millions of people by bringing together like-minded organizations to increase access to high-quality, value-based care.[3]

Kaiser Permanente has a long history of leveraging technology to support our fully integrated, value-based model of care and coverage. Through the value-based platform we are developing with Risant Health, we leverage our clinical knowledge and technology tools to bring evidence-based care protocols to providers and consumers to improve health outcomes and lower costs. As health IT continues to rapidly evolve, Kaiser Permanente approaches digital transformation through the lens of value-based care and we appreciate efforts by CMS and ASTP/ONC modernize the health information technology infrastructure.

In addition to our more detailed comments below, we ask that the administration pursue the following high-priority policy actions:

---

[1] 90 Fed. Reg. 21034 (May 16, 2025).

[2] Kaiser Permanente comprises Kaiser Foundation Health Plan, Inc., one of the nation's largest not-for-profit health plans, and its health plan subsidiaries outside California and Hawaii; the not-for-profit Kaiser Foundation Hospitals, which operates 40 hospitals and more than 600 other clinical facilities; and the Permanente Medical Groups, self-governed physician group practices that exclusively contract with Kaiser Foundation Health Plan and its health plan subsidiaries to meet the health needs of Kaiser Permanente's members.

[3] Risant Health currently provides high-quality, value-based care to more than 3 million patients and members.

- Improve identity verification processes through a decentralized, privacy-preserving standards-based digital identity framework that enables payers and providers to jointly authenticate individuals and participate in trust ecosystems, without requiring use of intermediaries.

- Develop a standards-based, open access directory that includes validated Health Level Seven International (HL7) Fast Healthcare Interoperability Resources (FHIR) standard endpoints, identity credentials, trust anchors, status of participation in the Trusted Exchange Framework and Common Agreement (TEFCA) and network affiliation to support health plan provider directories, patient health care data sharing and health care business transactions.

- Build upon TEFCA to support expanded data sharing purposes across and among federal agencies, health care entities, apps, and individuals. Expanded purposes should include clinical research, health care quality and patient safety reporting, public and population health, health care payment and risk reporting.

- Improve electronic prior authorization (PA) and other administrative transaction processes by providing payers and providers flexibility to use recognized alternative standards to outdated Health Information Portability and Accountability Act of 1996 (HIPAA) administrative transaction standards.

The health care interoperability landscape is rapidly evolving, driven by technological advancements, regulatory changes and a growing emphasis on patient-centric care. A coordinated approach is essential to maximize the benefits and minimize the administrative burden and costs associated with adopting and maintaining new technology. We recommend that CMS and ASTP/ONC collaborate with the health care industry to select a few high-priority process improvement opportunities. This will focus efforts and provide sufficient time for health care payers and providers to develop, test and implement technical solutions. We also recommend that CMS and ASTP/ONC work together to develop a coordinated interoperability implementation plan and roadmap that accounts for all changes to standards and exchange requirements across federal agencies to ensure inter-dependencies are appropriately managed and prevent unnecessary administrative burden and implementation costs.

API IMPLEMENTATION

FHIR based application programming interface (API) solutions enable lower cost and more flexible real-time access to data, facilitate seamless integration with various health care IT systems and support technological innovation to improve patient care and outcomes. However, fragmented implementation timelines, lack of coordinated technical guidance and minimal integration with quality or network performance programs impede broad adoption.

To encourage greater uptake, we recommend that CMS incentivize participation across the Medicare, Medicaid and qualified health plan (QHP) programs. CMS should also publish ASTP/ONC reference implementations for FHIR-based APIs that payers and providers can leverage to ease implementation. Finally, CMS should continue to enhance Blue Button 2.0 and Data at the Point of Care as examples of foundational infrastructure for the digital health care ecosystem.

Patient Access API

The patient access API allows patients to access and share information like claims, encounter details and clinical data. However, many patients are unfamiliar with the technology and do not understand how to use it. CMS could develop programs to educate patients about how APIs can help them take a more active role in their care. This education campaign could also include information about privacy concerns and risks posed by third-party apps and how to evaluate information sharing requests.

Prior Authorization API

We support efforts by CMS to offer technological solutions that reduce administrative burden associated with prior authorization; however, meeting the 1/1/2027 compliance deadline (CMS Interoperability and Prior Authorization final rule) may not be possible due to anticipated developer and vendor delays, which will compress the amount of time for payers to test and implement. Also, it is unclear whether vendors are currently able to build the necessary reciprocal interfaces to allow the EHR systems used by providers to connect with the PA APIs being built by payers. This connectivity between the PA APIs and electronic health records (EHR) used by providers is crucial to realize the functionality and utility of the PA API.

Therefore, we recommend that CMS delay the compliance dates for the PA API requirements by one year to ensure payers have sufficient time to test and validate the APIs. This delay would also allow time for vendors to develop solutions to integrate the APIs with provider EHRs, to facilitate and promote provider adoption. Reporting requirements under the Medicare Promoting Interoperability and MIPS programs for providers to use the PA APIs should follow at least one full year after the newly revised payer deadline. For example, if the payer compliance deadline is extended to 1/1/2028, then any provider reporting requirements should not be required until 2029 or later.

We also recommend that CMS delay or revise FHIR based Documentation Templates and Rules (DTR), which is intended to ensure that documentation requirements for PA are met. However, the standard's lack of maturity may contribute to systems issues and instability during implementation. DTR, in its current form, imposes a substantial implementation burden on integrated systems like Kaiser Permanente without a corresponding benefit for providers or patients. We recommend that CMS delay this provision until the standard matures and has been tested and validated in a variety of environments.

Electronic Health Information (EHI)

Full EHI Access. We do not support and recommend against incorporating full EHI access within APIs. We are concerned that the full EHI contains far too much information and would create costly technical issues along with significant potential privacy concerns due to the large amount of data contained in the EHI and the inability to account for individual patient preferences and state privacy requirements.

Standardizing Patient Level EHI Export. We do not support specifying standardized API requirements to support patient level EHI exports. Patients generally are not interested in this

functionality or format, and we are concerned that it will not be a good use of health care provider time and resources.

DIGITAL HEALTH TOOLS AND PRODUCTS

Access to digital health tools and products empowers patients and caregivers to take an active role in managing their health. CMS can encourage greater adoption by developing a certification program that allows patients to identify digital health tools and products that can connect through TEFCA to meet national standards for privacy, security, accessibility and interoperability. The certification program should enable patients to compare tools and provide a ranking of important features (e.g., language support) and also explain benefits of use, such as reduced out-of-pocket costs, faster appointment scheduling or proactive reminders for care.

We also recommend that CMS study the relationship between patient digital tool adoption and health outcomes and consider including incentives for providers and payers that offer access to digital tools and products that improve individual health outcomes.

DATA SHARING

Information Blocking

The 21st Century Cures Act directed ASTP/ONC to implement a process for payers and patients to report claims of possible information blocking. Unfortunately, many payers hesitate to report potential violations, while patients are often confused about what qualifies as information blocking.

We recommend that ASTP/ONC work with payers to develop and implement a structured complaint process that includes anonymous submission options, secure follow-up protocols and good-faith resolution pathways. We also recommend that CMS and ASTP/ONC provide education, issue technical assistance letters and establish reasonable cure periods for all actors, aligned with protections currently available to certified health IT developers. Patients would benefit from materials that clearly explain what information blocking is and what steps patients can take to access or share their information.

We also recommend that ASTP/ONC share anonymized details from information blocking complaints received to date to help providers and EHR developers and vendors understand the issues other actors are experiencing to design proactive solutions. However, we do not support any potential proposals that would require providers to develop custom solutions for requesters and instead recommend permitting providers to continue to leverage generally beneficial data sharing capabilities.

We do not support and recommend against eliminating any of the current information blocking exceptions. Instead, we recommend that ASTP/ONC revise the infeasibility exception to allow providers to post alerts on their website or patient portal stating that the provider is experiencing events beyond their control and is unable to fulfill requests rather than requiring the provider to send individual letters to each requester. This change will reduce administrative burden and cost

whenever a provider is unable to exchange data due to unavoidable events like natural disasters or cyberattacks.

Quality Reporting

Providers experience administrative burden when they submit quality reporting information to both CMS and payers, despite the availability of certified systems capable of extracting data directly. To address this, CMS should promote payer use of bulk FHIR APIs to extract clinical quality data, shifting the calculation burden away from providers. CMS and ASTP/ONC should work together to ensure certified health IT can support dual-purpose data reporting for use across MIPS, MA Stars, ACO programs and payer-specific analytics. We also recommend that CMS consolidate quality measurement requirements across programs and enable registry-based or automated payer calculation pathways—promoting "collect once, report many" functionality.

Modernize HIPAA Transactions

Currently, the HIPAA Administrative Simplification Provisions require all covered entities to use one standard and implementation specification to exchange data for each business function. This requirement, while previously helpful to ensure standardization, fails to keep pace with rapidly evolving technology and hinders innovation. Updating HIPAA transaction standards has been an unnecessarily long process and has delayed the ability of HIPAA covered entities to implement needed updates.

We recommend that CMS provide payers and providers flexibility to use recognized interoperable alternative standards in addition to HIPAA transaction standards to improve administrative efficiency, modernize health IT infrastructure and support value-based care models. This would not eliminate the existing HIPAA transaction standards but rather create a path for more efficient alternatives to be used. Without this flexibility, we are concerned that long delays experienced by HIPAA covered entities to update transaction standards will be exacerbated, contributing to increased costs and administrative burden for payers and providers.

For example, inefficiencies in exchanging prior authorization information can delay access to care. Permitting a more flexible standards approach would significantly accelerate industry adoption of more efficient administrative processes. We recommend starting with end-to-end FHIR based API transactions using HL7 Da Vinci FHIR standards and implementation guides as an alternative to existing HIPAA prior authorization exchange standards.

This approach would maintain existing baseline requirements for consistency purposes while enabling innovation. So long as a minimum standard (in this case the named HIPAA transaction standard and implementation specification) can also be met, willing trading partners should be allowed to implement any recognized alternative standard and implementation specification. To support this flexibility, CMS should develop an expedited approval process for these alternatives to current HIPAA administrative transaction standards.

NATIONWIDE PROVIDER DIRECTORY

Kaiser Permanente supports CMS seeking ways to improve provider directory accuracy and functionality, while reducing associated administrative burden. Accurate provider information is integral for patients and consumers to access care. However, provider information contained in existing systems is not reliable because it is not kept up to date consistently, contains inaccuracies, and is not consistent across different systems. We are concerned that these serious challenges will carry forward to future systems if not addressed proactively. We recommend that CMS first focus on ensuring data quality, defining role clarity and responsibilities, streamlining regulatory requirements and establishing accountable governance processes before implementing new infrastructure or interoperability requirements.

Data Quality

Accurate data is key to ensuring provider directories are functional and reliable. We recommend that CMS take the following steps to ensure that provider data is accurate and current before proceeding with any exchange mandates or directory expansion:

- Work with providers and payers to design and implement a comprehensive data quality improvement and management plan.

- Upgrade key sources of data (e.g., NPPES, licensure systems) to support new provider types, telehealth identifiers, and group affiliations.

- Define and implement a formal validation process to ensure ongoing accuracy of data (e.g., centralized federal contractor, payer attestation pipelines).

Defined Roles and Responsibilities

We recommend that CMS define technical and functional responsibilities for any directory operator or proxy, along with legal and regulatory safeguards for downstream users. We also recommend that CMS define and support the role of TEFCA and qualified health information networks (QHINs) in national directory services.

Design and Functionality

We support development of a standards-based, open access directory that includes validated FHIR endpoints, identity credentials, trust anchors and TEFCA participation status and network affiliation. These features would help resolve long-standing challenges to endpoint discovery and credential validation, while supporting efforts to replace fragmented infrastructure with scalable, standards-based platforms.

We recommend that a national provider directory function as a federated infrastructure that can aggregate and index authoritative data sources without replacing or duplicating public facing health plan provider directories. As provider directories can offer consumer-facing engagement and brand assets, stakeholders should retain operational control over their respective data (e.g., payers over network relationships, providers over practice locations).

We recommend CMS explore a model that utilizes certified intermediary entities (proxies or clearinghouses) to serve as routing infrastructure for FHIR-based data exchange. This would allow one-time integration per actor, support traceability and auditability, reduce the need for bilateral connections between trading partners and expedite administrative transactions without sacrificing integrity or scalability.

Phased Implementation with Use Case Alignment

We recommend that CMS phase implementation beginning with establishing the infrastructure necessary to support current interoperability requirements. Once that functionality is implemented, CMS should consider expanding in stages to other use cases beyond provider directories such as PA APIs, quality measure reporting, and public health and research data routing.

DIGITAL IDENTITY

Digital identity infrastructure can be used in health care to streamline administrative processes, improve access to health records and ensure data accuracy, leading to improved patient experiences and outcomes. Navigating multiple login systems adds administrative burden and complexity for patients and providers. Credential service providers (CSPs) can be used to streamline authentication processes; however, use of CSPs can also introduce privacy and security risks when used in health care. Emerging cryptographic technologies, including person-centric digital identities anchored to verified personal identifiers (e.g., identity wallets or cryptographic credentials using zero-knowledge proofs) are currently being piloted in other industries and offer scalable, privacy-preserving alternative to legacy credentialing systems such as CSPs.

We recommend that CMS and ONC/ASTP work with the National Institute of Standards and Technology (NIST) to develop a decentralized, standards-based health care identity framework that aligns with current digital identity and credentialing guidelines and frameworks[4,5] and enables payers and providers to authenticate individuals and participate in trust ecosystems, without requiring the use of intermediaries or third parties. This approach supports secure access and avoids requiring additional, unnecessary layers of manual attestations, or use of centralized credentialing models that introduce risk. Additionally, this framework should be flexible to accommodate various technologies (e.g., CSPs, cryptographic credentials) to ensure ongoing innovation and improvement in identity verification technologies and accommodate patient and provider preferences.

TEFCA

Clarify Role and Scope of TEFCA

The TEFCA network can reduce administrative burden for health care payers and providers and promote nationwide interoperability, leading to significant cost savings and improved patient outcomes. Unfortunately, at present, overlapping data exchange frameworks, limited utility for

---

[4] National Institute of Standards and Technology. (2024). *Digital Identity Guidelines Second Public Draft* (NIST Special Publication 800-63-4 2pd). https://doi.org/10.6028/NIST.SP.800-63-4.2pd
[5] National Institute of Standards and Technology. (2017). *Digital Identity Guidelines* (NIST Special Publication 800-63-3). https://doi.org/10.6028/NIST.SP.800-63-3

payers, narrow application of regulatory flexibilities for providers and slow development of additional use cases for the network collectively hinder fuller participation. To address these limitations, we recommend that CMS and ASTP take the following actions:

- Support bulk FHIR-based exchange
- Expand TEFCA's permitted purposes to include health care payment and operations to incentivize adoption by payers
- Further expand supported use cases to include research, public health, and vital statistics
- Revise the TEFCA information blocking exception to allow sender-only to qualify
- Leverage TEFCA participation to streamline existing exchange attestation requirements in interoperability program requirements to reduce duplicative compliance frameworks
- Expand use of TEFCA to connect individual patients and caregivers to applications that manage data sharing for health and wellness

We support leveraging TEFCA to support data sharing between and among federal agencies and health care entities to serve multiple purposes. For example, TEFCA supports efforts to expand value-based care by enabling effective care coordination, outcome measurement and risk management activities necessary to support value-based payment models. TEFCA can also be used to support public health reporting and surveillance activities between health care entities, local public health authorities and the Centers for Disease Control. Additional TEFCA use cases should be developed, with specifications published and maintained in coordination with federal agencies and private national health care accreditation organizations to support: health care quality and patient safety electronic measure reporting, public health electronic case reporting and syndromic surveillance reporting, vital statistics, including birth and mortality reporting and human subjects research authorized data sharing.

<p align="center">*   *   *</p>

Kaiser Permanente appreciates CMS and ASTP/ONC's consideration of our comments, and we look forward to continued collaboration. Please feel free to contact me at Jamie.Ferguson@kp.org or Megan Lane at Megan.A.Lane@kp.org with questions or if we can provide additional information.

Sincerely,

JAFergn

Jamie Ferguson
Vice President, Health IT Strategy and Policy
Kaiser Foundation Health Plan, Inc.