LEAVITT PARTNERS
An HMA Company

Robert F. Kennedy, Jr., Secretary
Dr. Mehmet Oz, Administrator
Tom Keane, Assistant Secretary and National Coordinator

Department of Health and Human Services
Centers for Medicare & Medicaid Services
Re: [CMS-0042-NC] RIN 0938-AV68: Request for Information; Health Technology Ecosystem

On behalf of Leavitt Partners, we are pleased to provide responses to this Request for Information. Leavitt Partners is a health care consulting firm with a special focus on digital health and interoperability. We work with organizations across all five of your categories, all of which have informed our thinking and feedback. We appreciate the opportunity to engage with HHS, CMS, and ASTP/ONC on these important issues.

B. Patients and Caregivers

1. Patient Needs

PC-1: What health management or care navigation apps would help you understand and manage your (or your loved ones) health needs, as well as the actions you should take?

a. What are the top things you would like to be able to do for your or your loved ones' health that can be enabled by digital health products?

The Leavitt Partners facilitated group, the CARIN Alliance has worked with a number of individual patients, consumers, and caregivers in addition to various organizations focused on consumer-access to health information. A number of priorities have been surfaced:

- Aggregating my health information and the health information of my family/dependants.
    - Using one login to access all of my providers so that critical information doesn't fall through the gaps due to human error or so I don't give up on aggregating my health information because I forget my login credentials.
    - Proving my identity one time instead of at every stop to reduce the number of steps required before access critical information, thereby decreasing the risk that my health information will be compromised.

    - Connecting to all of my providers through one digital tool to avoid "portalitis," decreasing my friction to access health information and increasing the likelihood that I will engage with my health data
        - Adding care partners of my choice through one digital tool, facilitating the ability of my spouse, children, or other care partner to help me coordinate and manage my health and health care.
    - Accessing images electronically through a more centralized format.
    - Accessing my claims information from my current and my past insurers, encouraging me to participate more fully as a health care consumer.
    - Receiving actionable updates and prompts, helping me better participate in my care.
- Scheduling appointments, reducing the friction to accessing my providers.
- Finding information about my costs (copays, deductibles, pricing ahead of procedures) and understanding my claims information, helping to make me a better health care consumer, avoid delays in care, and make sure I can afford my therapies.
- Finding providers in my health insurance network, helping ensure that I avoid out-of-network encounters and surprise medical expenses.
- Having the ability to share authoritative documentation like immunization registries, active medication lists and medication histories.
- Having the ability to easily ask my prescribing practitioner to refill my prescription.
- Having the ability to transfer my prescription order between different pharmacies to get the best price, based on my coverage.
- Having more information at my fingertips to evaluate cost and health care quality of different in-network and out-of-network providers.

b. If you had a personal assistant to support your health needs, what are the top things you would ask them to help with?

- Helping me get all of my health records into one place, including services I've received, medications that I need to take, appointments that are coming up, etc.
- Helping me understand my costs.
- Health navigator applications.
- Helping me navigate care and social needs outside of health care, including care management, social work needs, educational resources, etc.
- For patients with rare diseases or complex illnesses, helping me get second opinions or submit my health data for research.

As noted in our list in (a.) above, critical digital health capability for patients should include access to pharmacy clinical services beyond medication dispensing. Patients should be able to digitally coordinate with pharmacists who often have the most frequent patient interactions in healthcare. Specifically, patients should be able to:

- Access real-time pharmacy benefit information through standardized CARIN Consumer Real-time Pharmacy Benefit Check API.
- Share their health data with pharmacists for medication therapy management.
- Schedule and receive clinical pharmacy services through digital platforms.
- Have pharmacy-provided clinical services data incorporated into their comprehensive health record.

PC-2: Do you have easy access to your own and all your loved ones' health information in one location?

a. If so, what are some examples of benefits it has provided?

b. If not, in what contexts or for what workflows would it be most valuable to use one portal or system to access all such health information?

c. Were there particular data types that were unavailable? What are the obstacles to accessing your complete health information electronically?

The biggest challenges for consumer-directed health data access are:

- "Portalitis" (discussed elsewhere in our comments regarding digital identity).
- Token practices that require consumers to keep re-connecting their data, instead of giving consumers the option to "set and forget" their permissions till they decide to disconnect a connection.
    - Note that this may be a combination of vendor practices or provider choice; whatever the reason, it is important to remedy this issue to avoid "portalitis."
- Insufficient compliance with information blocking mandates to support patient access through HL7 FHIR-based APIs.
    - This is true for hospitals and MIPS-eligible clinicians and practice groups that are customers of certified API developers.
    - This is also true of other licensed health care practitioners, including non-HIPAA providers.
    - This is also true of labs, pharmacies, LTPAC providers and diagnostic imaging centers.
- The lack of a national mandate for all health plans to enable patient access APIs for members in their commercial lines of business.

- Insufficient access for active military service personnel and veterans to their clinical data from the military health system.
- The low volume of participants on trusted networks that actually respond to patient requests.
- The lack of a national health care directory that accurately represents the relationships of individual licensed practitioners to different practice groups and health systems, in a way that makes it easy for consumers to accurately locate all the right API endpoints they need to connect their data.

PC-3: Are you aware of health management, care navigation, or personal health record apps that would be useful to Medicare beneficiaries and their caregivers?

The CARIN Alliance, facilitated by Leavitt Partners, has organized the website, myhealthapplication.com to help consumers, caregivers, patients, and care partners find personal health records and other consumer-facing applications that have attested to industry best-practices for privacy, security, transparency, and consent through the CARIN Code of Conduct. These applications may have functions across the areas of health management, care navigation, and PHR functions. The website can help anyone, including Medicare beneficiaries, discover trusted applications that can connect them with their health data.

We note, however, that many Medicare and Medicaid beneficiaries, members of QHP plans, patients, care partners, and consumers do not know about many PHRs or the utility of using such a tool. Once these individuals become aware of such tools, they often have challenges using something other than a provider's patient portal or a plan's member portal. We encourage CMS to consider ways to incentivize plans and providers to educate their members and patients about the availability of consumer-access tools, beyond a patient or member portal, and to encourage their use. This could be done during open-enrollment each year or during a "Welcome to Medicare" or annual wellness visit or in the My Medicare Portal. It could be encouraged during a medication reconciliation visit or on during a virtual visit with provider. However CMS chooses to incent or require this education, it is critical to the success and adoption of digital health tools and individual access policy initiatives that individuals are informed of the functionality and utility of various digital tools as well as informed about the options available to them.

Medicare beneficiaries, who often manage multiple chronic conditions and complex medication regimens, would also benefit from apps using NCPDP, CARIN Blue Button®, and HL7® FHIR® standards to coordinate with their pharmacists. APICS is documenting and advancing successful

implementation models that demonstrate how pharmacy integration improves patient outcomes.

Pharmacists are currently isolated from broader health care teams and face limited access to comprehensive patient data despite their frequent interactions with patients. Applications that bridge this gap would allow Medicare beneficiaries to benefit from the clinical expertise of pharmacists who could provide medication therapy management, identify potential drug interactions, support medication adherence and provide chronic care related clinical services in accordance with their scope of practice when given proper access to patient data and integration with other providers.

PC-4: What features are missing from apps you use or that you are aware of today?

Some of the major challenges to consumer-facing tools' utility lies not with the functions that are or are not included in PHRs or other consumer-facing applications. It is important to note that the APIs needed to enable a number of functions that would benefit consumers are not available or are proprietary and locked--off behind technology vendor or provider paywalls. Seeing schedule availability, canceling, rebooking, messaging, requesting refills are all functions that must be enabled to ensure that consumer engagement is seamless and friction is reduced. Anything that patients can do in their EHR portal needs to have a matching open API to allow them to complete those functions in an application of their choice.

PC-5: What can CMS and its partners do to encourage patient and caregiver interest in these digital health products?

- CMS can update that Medicare Blue Button® 2.0 gives beneficiaries options to use a digital ID + "selfy" to demonstrate how it helps more beneficiaries connect their data at FHIR API endpoints.
- CMS can also make sure Medicare Blue Button 2.0 allows beneficiaries to set the period of duration for an app to connect data to one year or indefinitely, in addition to shorter durations.
- CMS can update its Conditions of Participation to require CMS-regulated participants to provide accurate, neutral, fact-based authoritative consumer education about their patient access rights via their choice of application, and maintain a gallery of third party applications that are already connected to their endpoints. They should attest that they have reviewed and as needed updated this gallery each quarter, similar to the way Certified API Developers are required to do with their service base URL listings.
- CMS can also require this education to include information about how consumers can submit a request if they want a connection through a particular application, and include a

link to a consumer-facing page that links back to the health tech complaint portal maintained by the ASTP/ONC.

- CMS can also lead the way by demonstrating on Medicare.gov how this education and functionality can be presented.
- CMS must re-evaluate the Promoting Interoperability Performance Category. It does not provide adequate incentive for ACOs and MIPS-eligible clinicians to activate patient access APIs. It should be table stakes. If they haven't activated their patient access APIs, make it an automatic 0 score for the entire category. Also, publish guidance that failure to activate these APIs is presumptively information blocking conduct.
- Update Medicare Advantage Conditions of Participation by requiring MAOs to post a link to a connected apps gallery in their STAR rating profile.
- As well, require MAOs to add requirements in the network contracts for their in-network providers to maintain accurate listings of their connected apps gallery, and to maintain active patient access APIs throughout the contract term.
- Update the CAHPS Survey with questions to beneficiaries to see if they are aware of their rights to connect their health data through their choice of application, both with their health plan and their in-network providers. Apply a strong weighting on this measure.
- Create additional payment adjustments for CMS-regulated organizations that implement standardized APIs that support interactivity with third party apps for more seamless shoppable experiences, including SMART Health Card for immunization records, active medication lists and medication histories, consumer real time pharmacy benefit check, and digital insurance card.
- Ensure the national health care directory being developed by CMS includes quality measures about individual licensed practitioners and medical practices, follows the Patient Brands and Endpoints sub-specification and provides updated specialty and sub-specialty codes that are confirmed by the preponderance of patients they see with specific complaints. This will help app developers more easily navigate patients and caregivers to the right care.

There are a number of challenges that consumers, patients, and caregivers have when using consumer-facing applications. Most of these challenges relate to the difficulty in connecting to the information that would be most useful to them. Many of these challenges could be addressed by CMS and its governmental partners, including:

- Mandating the use of a third-party credential or identity, and requiring EHRs, providers, and CMS-regulated payers to accept those credentials without additional steps. Many consumers suffer from "portalitis," having to remember countless user-names or passwords to login to each provider or payer. Using a "login with" function, with an IAL2 credential, would go far in alleviating these challenges.

- Consumer facing applications face a number of challenges when seeking to connect users to data sources. Many of these challenges have been catalogued with exhaustive detail by the app developer community within the CARIN Alliance.[1] Among these challenges, the more acute dynamics include:
    - FHIR endpoint discovery: Endpoint discovery is challenging. CMS and ASTP/ONC should aggregate and publish a FHIR endpoint directory.
    - Onboarding and registration: FHIR endpoint data holders are often slow to register and onboard consumer-facing applications. CARIN recommends several standardized approaches, consistent with the Interoperability and Patient Access Rule that should be mandated more universally
    - Ongoing support: Various technology vendors, including those that support providers and CMS-regulated payers, often struggle to support the standards-based APIs required for individual access queries. While entities subscribing to proprietary platforms or participating in specific application vendor programs at EHRs and payer systems get quick responses and fast fixes to technical issues, support for standards-based APIs can significantly lag.
- The lack of support for consumer-facing applications, and the challenges that these tools have in accessing, and maintaining access to, individual access endpoints, creates unnecessary friction for beneficiaries, patients, and caregivers. When that friction is encountered, these individuals often abandon the tools or give up trying to find and access the necessary data. CMS and ASTP/ONC must do more to require EHRs, payer technology systems, and the data holders themselves to support consumer access, including streamlining the ability of consumer facing applications to act on behalf of their users. The vision articulated in the CURES Act of consumer access to their information without special effort will not be realized until this is more of a reality.

a. What role, if any, should CMS have in reviewing or approving digital health products?

The certification of digital health products has progressed significantly since the passage of the HITECH Act. Similarly, products regulated by both CMS and ASTP/ONC have advanced significantly. We believe there is now an opportunity to change the way that certification occurs at both ASTP/ONC and CMS:

[1] See the CARIN Alliance webpage under Developer Resources; specifically "Patient Access APIs in the Wild: Challenges with Scaling User Choice Without Special Effort", "Endpoint Discovery", "Registration and Onboarding", "FHIR Standard APIs with Related Support and Enablement Services" and "Patient Experience" (forthcoming)

- ONC should change the definition of CEHRT (Certified Electronic Health Record technology) to "API CEHRT" (Application Programming Interface Certified Electronic Health Retrieval Technology).
- The ONC is able to redefine API CEHRT based on the original definition in the HITECH Act, which includes the adoption of standards in Section 3004 and defines health information technology as inclusive all of the "hardware, software, . . . or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information." This definition would include EHRs, LIS, RIS, payer systems, API vendors, and cloud-based solutions, in effect any HIT that supports some or all ePHI or EHI.
- API CEHRT should focus exclusively on certifying the HL7® FHIR® APIs that providers and payers send and receive and no longer certify the functionality within the EHRs or EDI X12 transactions.
- CMS should then point to the new definition of API CEHRT in their regulations to ensure consistency between providers and payers.
- The APIs on ONC's Inferno Test Kit website should be supported by payers and providers and implemented within the next two years.
    - We support the addition, within Inferno, to add service-level standards to API testing. Data should be present and confirmed as performant.
- Improve testing of production APIs by requiring the inclusion of a standard test patient in the production environment for all HL7 FHIR-based API, and publish detailed results of these automated tests publicly on Lantern every week (with a score out of 100).

b. What changes would enable timely access to high quality CMS and provider generated data on patients?

CMS should retain a light touch on app approval, but encourage attestation to codes of conduct (e.g., the CARIN Code of Conduct) that enable apps to declare a high bar for privacy and security. CMS could accept submissions of outcomes data associated with these apps, and publish the apps in a directory along with their outcomes data and code of conduct attestation (similar to CARIN's MyHealthApplication website).

We also note, though, that CMS should include patients and caregivers in the process of designing and disseminating digital health products in ways that make it easy for them to use and ensure that it provides meaningful information and support. Ideally, feedback opportunities for digital health products will involve patients with a wide range of health statuses and backgrounds (e.g., different diagnoses and different familiarities with technology). Overall, CMS should seek to ask patients and caregivers not only what data they would like from other stakeholders (i.e., CMS, plans, and providers), but what data they would like to send those stakeholders. In other words, CMS should be asking patients not only, "what data from

your doctor would you like to have," but also, "what would you like your doctor to know about you?"—this will be essential to building products that patients are interested in and can benefit from.

On the mental and behavioral health side, a coordinated federal approach is needed to evaluate Digital Mental Health Technologies and should consider the distinctions between general wellness technologies and those intended to screen, diagnose, support, treat, and monitor a mental health condition or SUD, which currently fall under FDA's device authorities.

Different evidence requirements across FDA, CMS, states, and other actors in the health care industry can present a barrier to DMHT advancement for startups and smaller companies. Insurers, employers, and other purchasers seek strong evidence on real-world effectiveness and impact on health outcomes and costs to make a decision on whether to pay for a product. This goes beyond the safety and efficacy considerations reviewed by FDA.

PC-6: What features are most important to make digital health products accessible and easy to use for Medicare beneficiaries and caregivers, particularly those with limited prior experience using digital tools and services?

As noted above, some of the biggest challenges that consumers, and especially Medicare beneficiaries, experience revolve around the friction that is created when trying to access health information. Challenges include remembering usernames and passwords, disparate data sources and the challenges of tools connecting to those data sources, incomplete data, and many more. As outlined above, we encourage CMS to consider ways to reduce the friction associated with connecting to providers and payers while increasing the utility of PHRs and other health navigation applications by making sure current regulations are followed by EHRs, providers, payer-technology vendors, and CMS-regulated insurers. We believe the specific use-cases outlined in PC-1 above, as well as things like prior authorization notifications for consumers, would have great utility for consumers and, specifically, Medicare beneficiaries and their caregivers.

PC-7: If CMS were to collect real-world data on digital health products' impact on health outcomes and related costs, what would be the best means of doing so?

As noted above, CMS could create a registry of health applications and request submissions of outcomes data tied to these apps. This could be as simple as a link to PubMed or other journal articles. AI could be used to summarize key points in a user-friendly way, or app owners could submit their own summaries.

CMS should also offer funding to support outcomes-related research involving digital health tools. CMS may also be able to see this in health tech partnerships and case studies that are written after treatment-control studies. CMS could put out a request for these.

2. Data Access and Integration

PC-8: In your experience, what health data is readily available and valuable to patients or their caregivers or both?

a. What data is valuable, but hard to access for appropriate and valuable use?

- Imaging data, including radiology images and pathology slides.
- After visit summary data, which is often not available via API access today.
- Claims data is available, but APIs are inconsistently implemented and difficult to access.

b. What are specific sources, other than claims and clinical data, that would be of highest value, and why?

Patient-reported data is demonstrated to have valuable uses for patients and providers but often is difficult for patients to submit to their providers and/or is not interoperable among providers on their care team. Ideally, patient-reported data (such as goals, symptoms, pain levels, etc.) should be submitted once by a patient and easily shareable across health systems and providers as part of a patient's medical record. The critical objectives, as it relates to patient-reported data, is a) minimizing the amount of times that patients need to submit the same information, and b) providing that information to all interested parties that could take advantage of knowing patient goals, symptoms, etc.

From an enrollment perspective, states are currently required to use data sources to verify financial information to the extent they determine them useful in determining Medicaid eligibility. In practice, states vary in their use of existing data sources to verify wages and net earnings from self-employment, unearned income, and resources using information from data sources such as the State Wage Information Collection Agency (SWICA), the Social Security Administration (SSA), state agencies administering state unemployment compensation, and human services programs.

CMS could utilize and support states in utilizing the National Directory of New Hires (NDHN) for Advanced Premium Tax Credit (APTC) eligibility determinations. The NDNH database includes information on newly hired and rehired employees, quarterly wage reports of existing employees, and Unemployment Insurance applications and claims. Created in 1996, this database is used by several "programs and agencies to verify program eligibility, prevent or end improper payments, collect overpayments, or ensure that program benefits are correct." According to the Congressional Research Service (CRS), "many programs that have piloted or

fully implemented the use of NDNH data to prevent improper payments have reported significant savings as a result." Multiple budget requests in 2017 and 2020 also proposed that CMS use the NDNH to support program integrity and "assist with income and employer verification and improve the ACA advance premium tax credit payment accuracy to reduce improper payments."

Importantly, adding NDNH data to the federal data services hub and encouraging states to utilize the database would reduce administrative burden on enrollees and states conducting redeterminations, and increase the number of people whose program eligibility can be verified without requiring duplicative and time-consuming paperwork from enrollees, processed manually by public agencies (ex parte). Specifically, according to CMS' data snapshot from December 2023 of Medicaid and CHIP enrollment, increased use of ex parte redeterminations during the unwinding period is correlated with smaller declines in enrollment among children under 19. Children were disproportionately impacted during the unwinding due to procedural denials, and ex parte renewals, built to scale, could prove to be a sustainable avenue to help individuals retain coverage and states to preserve capacity.

It is also important to note that under the current system, Advance Premium Tax Credit (APTC) eligibility determination relies on projected income, which can be difficult as individuals and families have to reasonably guess their future income. Projecting future income can be particularly difficult for workers engaging in the gig economy, part-time work, and seasonal labor, which are prone to income fluctuations. For example, one recent study found that nearly half of all low-income, working-age adults experience, each year, at least one month's spike in income that exceeds average monthly income by 25 percent or more. According to another study, the average low and moderate-income household experiences an average of 2.6 months per year in which income exceeds the family's annual income by 25 percent or more. Workers should not be penalized for reasonably anticipating a pay raise, additional hours at work, an increase in self-employment income, or finding a new job.

We also encourage the Trump Administration to work with Congress to utilize prior year income information, which can be verified through tax information and other sources, to establish eligibility for premium tax credits. Using prior-year income for premium tax credit eligibility would fundamentally address the accuracy and verification challenges with the current system. Please note this change should be coupled with opportunities for people whose circumstances have changed since their last tax return, such as through job loss, in a way that now makes them eligible.

Currently, there is significant variability in how and when states and the Exchange transfer information related to a Medicaid, CHIP, or Marketplace coverage application, and consumers can get bounced from program to program and asked many of the same eligibility questions by multiple government agencies. For example, the current account transfer technology utilizes an Extensible Markup Language (XML)-based data model with insufficient data quality controls, leading to incomplete and inaccurate data which can result in individuals having to fill out a new application with the Marketplace to receive an eligibility determination for Marketplace coverage. Additionally, states and the Marketplace routinely duplicate verifications when accounts are transferred.

Modernizing the technology and processes and standardizing enrollment files and information can significantly improve consumer experience and support accurate enrollments. The Enrollment Coalition encourages the Administration to engage states in a collaborative process to improve the technology facilitating transitions of coverage and accurate enrollment in coverage for which an individual is eligible.

Language in Section 1902(dd) of the Social Security Act eliminates the need for attestations under penalty of perjury when data from a "public agency" is used to establish an element of eligibility. CMS clarification that states can use, "A data match with the Department of Homeland Security (DHS) Systematic Alien Verification for Entitlements (SAVE) Program to verify citizenship and identity would reduce administrative burden to enrollees and increase accuracy." Relevant language is in 42 CFR § 435.407(a)(8)

c. What specific opportunities and challenges exist to improve accessibility, interoperability and integration of clinical data?

One opportunity for improving data integration is to support not only read access for patients but also structured, write-enabled interactions through trusted third-party applications and/or access to a patient's data on their app/portal of choice. This could allow individuals to submit and/or share home-monitoring data, self-reported health and medication updates, or preferences that inform care decisions. CMS could consider pathways to encourage bidirectional exchange as part of advancing consumer-facing API functionality and digital engagement.

PC-9: Given that the Blue Button® 2.0 API only includes basic patient demographic, Medicare coverage, and claims data, what additional CMS data sources do developers view as most valuable for inclusion in the API?

a. What difficulties are there in accessing or utilizing these data sources today?

The Blue Button 2.0 API currently only includes basic patient demographic, Medicare coverage, and claims data (Part A, B, D). This limited dataset prevents a comprehensive view of the patient's health status. Many data sources remain isolated in proprietary systems or are difficult to access.

b. What suggestions do you have to improve the Blue Button 2.0 API experience?

The Blue Button 2.0 API should be expanded to include additional data sources and adopt more advanced FHIR implementation guides. Specifically:

- Implement the APIs on ONC's Inferno Test Kit website for payers, including:
  - CARIN Consumer Real-time Pharmacy Benefit Check
  - CARIN Digital Insurance Card and API
  - Da Vinci Payer Data Exchange (PDex)
  - Da Vinci Plan Net
  - Da Vinci US Drug Formulary
- Improve developer support by providing a test sandbox, development environment, detailed technical documentation, and synthetic data for applications to test against.
- Validate conformance to the regulations by testing APIs against the ONC's Inferno Test Kits.

c. Is there non-CMS data that should be included in the API?

The Patient API should facilitate access to price transparency data, prescription benefit information, and provider directory information. Specifically, implementing the Patient Cost Transparency HL7® FHIR® API Implementation Guide to support the ability of patients to determine their out-of-pocket costs would be valuable.

CDC data could also be useful in some contexts, specifically in terms of particular risks of the user based on where they live and/or known condition. An example of this is COPD. If the CDC "knows" there is a flu breakout in user's location the issuance of a health alert to that user would be useful.

PC-10: How is the Trusted Exchange Framework and Common Agreement™ (TEFCA™) currently helping to advance patient access to health information in the real world?

TEFCA is moving closer toward becoming an operational, everyday system for health information exchange. TEFCA has established the necessary framework and governance structures (QHINs, Participants, and Subparticipants) that will enable nationwide health information exchange, including Individual Access Services (IAS). However, there are still significant challenges that limit the promise of IAS on TEFCA. As noted in other areas, identity management, patient matching, reciprocity expectations and other issues have slowed the adoption of IAS on TEFCA and limited the utility to patients and the tools they use.

The implementation of the 21st Century Cures Act, alongside TEFCA development, has pushed policy toward patient ownership of data. IAS within TEFCA will enable individuals, through the application of their choice, to query and obtain their medical records and other health information from multiple sources, including the ability to discover where their records may reside through record location technology.

a. Please provide specific examples.

- Under the Common Agreement, a participant or subparticipant data holder may decline to return records in response to an IAS request - even if the request generates a single patient match—if the participant/subparticipant's local matching rules have not been met. The rationale for this policy is that even with return of a single match in response to a query, there is no guarantee that the record is a 100% match—and participants/subparticipants perceive liability under HIPAA (or at least a requirement to notify) if there is a breach due to sending what turns out to be the wrong record.
- The CARIN Alliance (of which we are a member) and other key interoperability stakeholders have asked OCR for further HIPAA guidance on this issue, but to date no action has been taken.
- Consequently, one large certified EMR vendor is taking the position that response to individual access requests (IAS) through TEFCA should not include payload (actual records) but should instead be limited to a return of FHIR endpoints of locations for the patient's record; the patient would then need to connect to each FHIR endpoint in order to secure the payload. This places multiple steps in a process that should be seamless given other protections in place (required use of an approved IAL-2 credentialed service provider and submission of a token indicating that the patient has been successfully identity proofed at IAL & AAL 2).
- At the same time, at least one other certified electronic medical record provider has demonstrated return of payload in response to a compliant IAS query.

- CMS should use its authorities to incent or mandate the return of payload in response to an IAS query.
- To support this—and ease concerns of HIPAA provider data endpoints participating in TEFCA—HHS should issue guidance regarding liability for return of a wrong record even when safeguards are followed.

b. What changes would you suggest?

To advance TEFCA implementation for patient access, we recommend:

- Implement standardized identity proofing using IAL2 credentialing with NIST 800-63-3 standards and the CARIN Credential Policy for trust alignment, with federation via UDAP Trust Community.
- Require all Designated QHINs to complete cross-network IAS testing on both sides of IHE Document Exchange APIs (that is, as a requesting and responding QHIN) within 12 months of signing the Common Agreement, and similarly with HL7 FHIR-based APIs as they are being deployed.
- Update the RCE's QHIN Participant/Sub-Participant Directory with information indicating which OIDs are responding to IAS Queries, and which have successfully responded with records for IAS purposes, and make time-stamped histories of IAS responses query-able. Also, support interoperability between the RLS directory and the national digital healthcare directory that CMS wants to build. More transparency exists if the RLS accurately represents the parent-child relationships of affiliated OIDs. Make the RLS Directory public.
- Modify the TEFCA governance structure to ensure more representation by IASPs, specifically on the Governing Council, and the Participant/Subparticipant Caucus.
- Clarify that TEFCA's reciprocity requirements are different for non-HIPAA IASPs than for other Participants and Sub-Participants. The TEFCA Terms of Participation v1.0 (April 2024) and TEFCA Exchange Purpose SOP v4.0 (January 16, 2025) make clear that IASPs that are Non-HIPAA Entities are not required to respond, but given the stance that several QHINs are taking, we believe a crystal clear policy clarification is needed, to remove conditions of reciprocity as a current barrier to wider IAS exchange on TEFCA. TEFCA OCR has long-standing guidance that patient requests cannot be conditioned on acceptance of other obligations.[2] IASPs have a choice whether to support reciprocal exchange, but that must be with the patient's consent.
- Work with OCR to update the TEFCA Common Agreement and TEFCA Security Incident Reporting SOP v1.0 (July 1, 2024) to clarify that all wrong records shared over networks and exchanges with Requestors (including IASPs) are always considered breaches, but are also subject to the low probability of compromise analysis. That means all Requestors have a duty to report wrong records to Responders, not just IASPs. Under the low probability of compromise, guidance should explain how the breach is not reportable when IASPs and other responders sign onto the Terms of Participation, which require among other things that Non-HIPAA Entities accept relevant standards set forth in the HIPAA Security Rule, HIPAA Privacy Rule and HIPAA Breach Notification Rule. Notably, the same analysis will

[2] For example (Private practice may not condition a patient's access to PHI on an agreement not to publish commentary about the practice) https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/all-cases/index.html

support exchange for public health purposes and government benefits determination as well. CARIN Alliance has engaged the ASTP/ONC staff repeatedly on this topic in 2024 and before that engaged the OCR staff as recently as December 2022. The next step is for OCR to be re-engaged, to consider our analysis, and take action with policy guidance or rulemaking.

- TEFCA's ultimate viability depends on trust, which depends most on transparency and individual participation. We endorse recommendations from Josh Mandel: For TEFCA to earn public trust and achieve widespread adoption, it must be designed from the ground up with robust, user-friendly mechanisms for individual transparency (knowing who accessed their data) and control (managing how it's shared) at the network level, with corresponding obligations for participating EHRs to honor these preferences. IAS serves as the great "unlock" for public trust to be achieved and maintained.
- Address privacy & consent management capabilities using identity-linked consent artifacts, OAuth 2.0-based user-managed authorization flows, and federated consent via UDAP Authorization Extension Objects.
- Simplify technical integration through SMART on HL7® FHIR® for initial access, UDAP Dynamic Client Registration for scalable onboarding, and certificate-based client identity with digital certificate validation.
- Reduce privacy and security compliance burdens by adopting HL7® FAST Security IG, implementing UDAP JWT-based client authentication, and using privacy-protective attribute release.
- Improve patient trust through reusable IAL2 credentials from certified CSPs, implementing the CARIN Credential Policy for policy equivalency, and supporting multiple authentication pathways.
- Establish credential federation, allowing digital identities verified by one Credential Service Provider to be accepted by a FHIR endpoint that uses its own or a different Credential Service Provider without requiring duplicate identity verification. The HL7 FAST Security and Identity IGs provide stakeholder consensus-based approaches to this.

c. What use cases could have a significant impact if implemented through TEFCA?

High-impact use cases for TEFCA implementation include:

- IAL2 credential with Record Locator Services using SMART on HL7 FHIR EHR portal authentication, enabling consumers to access health information across multiple provider portals with a single credential.
- IAL2 credential with XCPD demographics match across multiple Health Information Exchanges, creating a single credential usable across multiple health information networks.

- IAL2 credential using OpenID Connect with single or multiple QHINs, returning either CDA or FHIR resources to IAS Providers, streamlining authentication and supporting both document and API-based access.
- Facilitated FHIR using HL7 FAST Security Implementation Guide, allowing QHINs to return FHIR endpoints instead of data directly for secure querying.
- Facilitated FHIR with B2B User Authorization Extension Object, supporting complex authorization models across both consumer and business use cases.
- Cross-provider credential acceptance demonstrating one credential issued by one CSP could be accepted by a FHIR endpoint that has not integrated that CSP into its system, establishing true identity federation in health care.

TEFCA could unlock new value by supporting direct patient contributions to their health record using a combination of structured FHIR write transactions and other means for clinicians to access patient contributions, e.g., access to their PHR app/portal where direct writes are not appropriate For example, enabling a patient to upload medication adherence logs or self-reported health goals through an application of their choice—validated by a credentialed identity—could significantly enhance data completeness and enable more personalized care planning, especially for chronic disease management.

A lot of angst expended over purpose of use and downstream secondary use can be resolved through consumer-mediated health data access and sharing. Consumer-directed access and exchange is a huge “unlock” for secondary uses like clinical trial matching and life insurance underwriting and post-market surveillance. But consumers are understandably concerned about “dark” data flows. Transparency for patients through individual access will help us move forward with network-based exchange for health care operations and other permitted HIPAA uses.

d. What standards are currently working well to advance access and existing exchange purposes?

Several standards work well for health information exchange, though not all are fully implemented within TEFCA yet:

- SMART on FHIR is widely implemented across the industry and provides immediate feasibility for IAS exchange.
- OAuth 2.0 technologies effectively support IAL2 credentials aligned with NIST requirements.
- The IHE Document Exchange XCPD API support secure, interoperable access for demographic matching between systems.

- The CARIN Alliance's work since 2016 has advanced consumer-directed exchange of health information and digital identity solutions.

e. What standards are not currently in wide use, but could improve data access and integration?

Promising emerging standards that could significantly improve data access include:

- HL7 FAST Security (required standard by January 1, 2026, under TEFCA) offers improved capabilities including certificate-based authentication and enhanced security controls.
- HL7 FAST Identity includes requirements for creating, managing, and federating Digital Identity including a Digital Identifier, as well as best practice patient matching, leveraging the certificate-based trust in HL7 FAST Security.
- OpenID Connect Federation 1.0 enables credential federation across different service providers.
- NIST 800-63-3 IAL2 compliant credentials, PKI certificate validation, and signed JWTs with authorization extension objects strengthen confidence in who has been authenticated.
- The NCPDP Patient Experience Identifier improves patient matching without compromising privacy.
- UDAP Dynamic Client Registration enables scalable onboarding of applications.

f. Are there redundant standards, protocols, or channels that should be consolidated?

Areas needing consolidation include:

- Fragmented identity verification standards across QHINs, Participants, and Subparticipants create redundant verification processes.
- Non-standardized acceptance of IAL2 credentials creates unnecessary friction for consumers accessing health information across multiple systems.
- The TEFCA technical framework needs standardized methods for passing authenticated credentials between QHINs. Toward this end, accreditation/certification bodies should publish the endpoints for keys used exclusively to sign services that meet accreditation requirements (consistent with each pairing of IAL/AAL, or higher, the relying party may desire), along with plain language stating that minimum identity and authentication assurance for which a key at that endpoint can be relied upon, as part of identifying who the accredited party is and when the accredited service is being used, to increase confidence in the binding to an identity issued by a certified Identity Provider.
- Different trust frameworks (Carequality, DirectTrust) need a common credentialing policy establishing equivalency through standardized requirements for IAL2 OAuth and PKI credentials.

g. Are there adequate alternatives outside of TEFCA for achieving widespread patient access to their health information?

Direct connections via standard FHIR APIs have worked well to bootstrap the industry; however, it's still complex for digital health tools to connect to thousands of disparate endpoints. Thus, the need for a single endpoint that enables patients to access all of their data in a standard and reliable way is pressing.

PC-11: How are health information exchanges (HIEs) currently helping to advance patient access to health information in the real world?

CyncHealth operates advanced HIEs and Prescription Drug Monitoring Programs (PDMPs) in Nebraska and Iowa. One example of their high-performing models is the ability to report on available hospital bed capacity in real time. In addition, Nebraska's PDMP is arguably the nation's only true medication reconciliation tool, promoting safer, more efficient care.

UHIN has also been very helpful in advancing a number of pilot efforts undertaken by the OneUtah Health Collaborative's digital health pilot. While some of these are adjacent to consumer-access, things like real-time e-Prior Authorization has a number of upsides for individuals.

PC-12: What are the most valuable operational health data use cases for patients and caregivers that would create more efficient care navigation or eliminate barriers to competition among providers or both?

A highly valuable but underused workflow is digital presentation of insurance coverage during appointment scheduling. A standardized, QR-enabled insurance card format would allow for instantaneous eligibility confirmation, helping patients avoid surprises related to coverage and network status. CMS could support this by naming a national digital insurance card standard and encouraging health plans to implement it via their Patient Access API infrastructure. Additional advancements on good faith estimates and advanced EOBs are also crucial for patients to understand what their out-of-pocket costs are likely to be at the time of scheduling, rather than at the time-of-service delivery.

A critical operational use case is enabling patients to track the status of prior authorization requests via third-party apps or health plan portals. Delays and lack of transparency in the PA process often result in care disruptions. CMS should encourage implementation of standardized APIs that allow consumers to view the status, rationale, and estimated decision timelines for pending authorizations. CARIN and the Da Vinci Project have been exploring this consumer-focused workflow, which builds on CMS-0057-F principles of transparency and real-time data exchange.

Additionally, CMS should work to enable users to share their patient-generated health data with their care team in standard ways (see feedback above about standard ways to write data back to the EHR and/or access to the patient's data on their app/portal of choice). This may include information such as:

- Activity
- Sleep quality
- Lab results from external sources
- Links to images
- Alerts about potential illness (or other regulated features)

We also note the high value of operational data in the pharmacy space. High value use cases include:

- Access to real-time out-of-pocket costs through CARIN Consumer Real-time Pharmacy Benefit Check
- Digital insurance card sharing using CARIN IG for Digital Insurance Card FHIR API
- Integration of pharmacy clinical services data with comprehensive patient records
- Pharmacist access to clinical data enabling more informed clinical services and medication therapy management

These use cases would eliminate barriers to competition among providers in several important ways:

First, by enabling real-time pharmacy benefit information through standardized APIs, patients gain price transparency across different pharmacy providers, fostering competition based on both cost and service quality.

Second, standardized documentation for pharmacy clinical services would allow patients to make informed choices between pharmacist-provided care and similar services offered by other provider types, creating a more level competitive field.

Third, incorporating pharmacy-generated clinical data into comprehensive patient records would enable pharmacists to compete more effectively as clinical providers rather than being limited to dispensing roles.

By removing these information barriers through standardized data exchange, patients gain more provider options and can make care decisions based on quality, convenience, and cost rather than being restricted by technological limitations and information silos.

a. Examples may include binding cost estimates, viewing provider schedule availability, etc.

b. What use cases are possible today?

c. What should be possible in the near future?

d. What would be very valuable but may be very hard to achieve?

Additionally, The National Council for Prescription Drug Programs' "Industry Guidance for Implementation of Admit, Discharge, and Transfer Notifications for Pharmacy" (Version 10, November 2024) identifies several high-value use cases that would significantly improve patient care coordination and safety if implemented broadly. A critical operational gap exists in the current healthcare ecosystem: pharmacies are often excluded from receiving ADT notifications despite being integral to medication management.

The NCPDP white paper clearly recommends that the pharmacy of record should be designated as a required recipient of ADT notifications, supporting several valuable operational use cases:

- Medication Reconciliation Post-Discharge: "Upon receiving an ADT notification about a patient's discharge, pharmacists can reconcile discharge medications with existing medication records. This process helps avoid duplications, omissions or harmful interactions, significantly enhancing patient safety and reducing readmission rates" (page 10). This creates more efficient care navigation by proactively preventing medication errors during transitions of care.
- Continuity of Care for Treatments: ADT notifications enable "pharmacists to coordinate with healthcare providers to ensure uninterrupted access to necessary medications" (page 10), which is particularly critical for patients with chronic conditions requiring consistent medication regimens.
- Auto-Refill and Medication Synchronization Management: "For patients admitted to hospital inpatient settings, it is often necessary to temporarily halt automatic medication refills and synchronization services. ADT notifications alert pharmacies to these admissions, allowing them to suspend these services during the inpatient stay. This prevents unnecessary medication dispensing and ensures medication lists are accurate upon the patient's discharge" (page 11).

These use cases directly address the intent of this question by:

- Creating more efficient care navigation through timely notification of care transitions.
- Eliminating barriers to competition by ensuring all pharmacies, regardless of size or affiliation, can participate in care coordination.

- Reducing fragmentation in care by including pharmacists as active participants in the patient's care journey.

While current technology can potentially enable these use cases today, policies and implementation guidance should be updated to explicitly include the pharmacy of record as a required recipient of ADT notifications.

3. Information Blocking and Digital Identity

PC-13: How can CMS encourage patients and caregivers to submit information blocking complaints to ASTP/ONC's Information Blocking Portal? What would be the impact?

CMS can boost beneficiary-directed education on Medicare.gov about their right to submit government complaints if their health care providers or MAOs don't allow them access to their electronic health information through their choice of application.

CMS can add a link to a consumer-friendly complaint portal on Medicare.gov for authenticated beneficiaries, which links on the backend to ASTP/ONC's Info Blocking Portal.

CMS can require CMS-regulated payers to deliver similar education to Medicare beneficiaries, Medicaid enrollees and QHP members and include the same link on the home page of their member portals or the plan's home page.

Increased reporting would almost certainly improve consumer-directed data exchange. A good proof point is how HIPAA covered entity compliance with 45 CFR 164.524 has increased in direct response to stepped up OCR's investigation and enforcement of HIPAA individual access complaints. Also, publishing and maintaining a scorecard causes covered entities to prioritize compliance, evidenced by a study conducted after Citizen Health first produced its individual access scorecard in 2019. Increased reporting aligns with the truism: "what doesn't get measured, and publicly reported, doesn't get improved."

PC-14: Regarding digital identity credentials:

a. What are the challenges today in getting patients/caregivers to sign up and use digital identity credentials?

The primary challenges today include fragmentation of identity systems across health care, lack of standardization, and the complexity of managing multiple credentials. Additionally, the limited ability to use a single digital credential means patients often have to sign up over and over again.

Patients currently navigate a disjointed set of portals to access their health information, making it nearly impossible to proactively manage their health information across different providers

and systems. This creates significant downstream issues in identifying individuals across systems, costing the healthcare system millions of dollars.

Another often forgotten challenge is the power of trust, and what happens when patients have low-trust in the systems they interact with. With so many fragmented identity systems, today's certification standards don't leave users confident in the operator of a sign-in page presented to them. Of course they don't complete the flow. With one trusted source (i.e., one Credential Service Provider that each patient or authorized representative elects to use, of the many choices available–or is offered as part of IAS–and some may elect to use more than one) that patients can start recognizing, we will be on our way to significantly less resistance to data sharing.

If digital identity credentials were more widely used, individuals could more accurately and efficiently enroll in programs they are eligible for, such as Medicaid, CHIP, or ACA plans. Wider use of digital identity credentials would also strengthen program integrity and make it easier to validate or re-validate criteria such as income, employment, and citizenship. Opening the federal data services hub API is critical to unlocking this potential fully.

b. What could be the benefits if digital identity credentials were more widely used?

Federated credentials would dramatically reduce friction in accessing health information across portals, apps, and networks. Adopting standardized digital identity credentials would dramatically improve patient access by enabling a single identity across providers and payers. It also is a better security model (many portals have not yet updated their systems to a strong identity assurance minimum bar with multi-factor authentication, as required by the HL7 FAST Identity IG) while limiting the likelihood of patient lockout (a commercial CSP may be better-equipped to enable 24x7 support for forgotten credentials when escalating to repeated identity verification is potentially needed).

Federated credentials would allow patients to create their own single digital identity, aggregate their own health information with an application of their choice, and provide their insurance information digitally, eliminating redundant paperwork and improving care coordination.

c. What are the potential downsides?

As these proposals are implemented, we need the technology to be easily accessible to everyone, including those who live in underserved communities, lack strong technology knowledge themselves, or struggle to obtain and maintain valid forms of government ID.

Additionally, many stakeholders that Leavitt Partners works with have expressed concerns about data misuse. While the promise of digital identities for various interventions is high, concern remains about how data linked to housing insecurity, mental and behavioral health, and other issues may be used.

d. How would encouraging the use of CSPs improve access to health information?

Widespread implementation of Credentialing Service Providers would eliminate the need for separate authentication systems at each provider and payer. This would streamline access to health information by accepting a NIST 800-63-3 IAL2 or higher certified identity provider as valid for a consumer to access their data and to create a login session using OpenID Connect, with data provided via an openly provided API.

e. What role should CMS/payers, providers, and app developers have in driving adoption?

CMS/Payers: Require implementation of NIST 800-63-3 IAL2 standards for identity verification and authentication and incentivize the adoption of identity federation across health systems.

Providers: Accept verified digital identities from certified IAL2 providers rather than maintaining separate identity systems. To successfully deploy digital identity credentials, healthcare organizations, payers, etc. who are managing identities today need to modify their systems to organize their records on unique identities, so that demographics that are shared in an ID token from Digital Identity/reusable credentials can confidently be "matched" to the correct person within their system. Otherwise, we have strong security in a credential that may be reused, but that credential may be allowed access to a different person's personal information and health data than is appropriate. The HL7® FAST Identity IG provides guidance on this topic, whether IdP integrations are done as one-off, more scalably integrated according to PKI-based trust via UDAP Tiered OAuth (securing CSP trust via PKI-based validation), or somewhere in-between.

App Developers: Incorporate standards like OpenID Connect and support identity federation.

f. How can CMS encourage patients to get digital identity credentials?

CMS should require that any system used for registration and login to access data on any health care network follow the NIST 800-63-3 digital identity guidelines for identity assurance level 2 (IAL2) and authenticator assurance level 2 (AAL2) for patient and provider identity and authentication. This requirement could be implemented within certification programs for providers and payers.

We encourage CMS to consider how it can leverage current federal and state government processes and functions, including login.gov (especially for VA use cases!) and state-level mDL/eDL efforts. Where a user has a government secured and verified identity they should be able to use that to prove identity for medical records access AND portal login.

Respectfully Submitted:
Ryan Howells, Principal
David Lee, Principal