Re: CMS and ASTP/ONCs Request for Information; Health Technology Ecosystem (CMS-0042-NC)

On behalf of CommonWell Health Alliance, we are pleased to submit comments on CMS and ASTP/ONCs Request for Information; Health Technology Ecosystem (CMS-0042-NC) published on May 16th, 2025.

CommonWell Health Alliance is a not-for-profit trade association that includes a variety of health IT and health care stakeholders. We work on interoperability across technology companies, payers, agencies, providers, clearing houses, patients, and more. Since our launch in 2013 with services focused on Care Treatment, we have enabled other use cases including Individual Access and look forward to furthering adoption and expansion of existing and future use cases.

Our vision is simple: health data should be available to individuals and caregivers wherever care occurs, at a reasonable cost. CommonWell, with our service provider and members, has created a vendor-neutral platform to remove barriers to effective health data exchange. We leverage standards and policies to enable scalable, secure, and reliable interoperability for our members and their customers nationwide.

Special Note Regarding Our Comments

These comments are reflective of the opinions of the Alliance and its members in regard to the objectives of CommonWell. It is not intended to represent the individual comments of each of our Members. Comments made here are not intended to represent the view of any particular member; and we expect some of our members to submit their own comment letters.

On behalf of the CommonWell Health Alliance, thank you again for the opportunity to comment on the RFI. We look forward to next steps and continued partnership.

Sincerely,

Paul L Wilder
Executive Director
CommonWell Health Alliance
75 Arlington Street, Suite 500
Boston, MA 02116
paul@commonwellalliance.org

Federal Register :: Request for Information; Health Technology Ecosystem

E. Technology Vendors, Data Providers, and Networks

This section is intended for all stakeholders to provide input on questions as they relate to use cases and workflows that involve technology vendors, data providers, and networks. While we certainly want technology vendors, data providers, and networks to answer questions in this section (and in other sections) from their point of view, we also invite all stakeholders to provide their viewpoints on the technology vendor, data provider, and network use cases as appropriate.

1. Ecosystem

TD-1. What short term (in the next 2 years) and longer-term steps can CMS take to stimulate developer interest in building digital health products for Medicare beneficiaries and caregivers?

TD-2. Regarding CMS Data, to stimulate developer interest—

a. What additional data would be most valuable if made available through CMS APIs?

b. What data sources are most valuable alongside the data available through the Blue Button 2.0 API?

c. What obstacles prevent accessing these data sources today?

d. What other APIs should CMS and ASTP/ONC consider including in program policies to unleash innovation and support patients and providers?

> Full support for Individual Access Services is essential. It remains challenging to obtain data from certain data-holding systems to the user's preferred applications. Most digital health tools will fail without accurate clinical data for the user or patient of the app. Although many apps exist, several potential apps are not developed due to developers' awareness of data access difficulties, leading them to refrain from creating new solutions. Manual entry by users is prone to gaps and errors, and compelling users to collect and upload all information themselves is impractical and labor-intensive. If data access were more straightforward, apps could improve and compete based on features and functionality.
>
> When I sought an app to manage my work, personal, and family calendars on my mobile device, I downloaded five different options before settling on the one that suited me best. It is uncommon for users not to trial apps—whether free or paid—before selecting a permanent option. Investing weeks or months to transfer data from provider systems to an app discourages experimentation, thereby limiting user engagement and developer innovation. This cycle must be broken to progress beyond the early adopter stage for health-focused apps.
>
> Furthermore, we believe that OAuth Authorization Code Flow, requiring the patient to log in to their portal(s), as a means to aggregate data from EHR-tethered patient portals, is insufficient to advance our goals. Patients often lack and or don't recall various portal

credentials for all locations where their data resides and may not even be fully aware of all data repositories. Anecdotally from our consumer application members, we have heard that 70% of users quit the process when presented with their portal login screen to access their data via the app of their choice. Even with comprehensive directories listing every interoperability endpoint nationally, challenges persist. Provider practices have various ownership and naming conventions, leading to discrepancies between practice names known by patients and those listed in directories. Additionally, practices consolidate, split, and change ownership over time, further complicating the matter.

Patients may also have forgotten or misplaced data from previous practices. They frequently move, change health plans, and switch practices, often unaware of the significance of older data for their current care. It is possible that they never even received access to a portal while getting care, therefore not having a credential to use to login effectively. While the relevance of clinical data diminishes over time for most conditions, this is not universally true. Patients should have an easier way to collect and manage all their data, enabling them to participate in health data exchange networks and frameworks with the same data flows available to their providers.

We strongly advise that ASTP/ONC provide incentives for developers to use the FAST Security for Scalable Registration, Authentication, and Authorization V1.1.0 as a starting point for allowing patients to leverage applications without needing their portal credentials. The FAST Security IG outlines a Tiered OAuth model that removes manual burden from the FHIR data query process and allows systems inside trusted networks to process requests.

Regarding directory improvement, we support CMS's initiative to develop a better national directory for interoperability. As a national exchange network with over a decade of experience, we recognize that current provider directories often misalign with goals and lack accurate and up-to-date information. We advocate for the creation of a comprehensive directory and encourage APIs for effective data exchange.

However, we advise caution in developing a directory that is too focused on individual providers and recommend prioritizing corporate identity. Data exchange (interoperability) and many administrative and clinical functions occur at the practice (organizational) level, not the individual provider level. For instance, when a provider retires or departs from a practice, their patient's records and obligations remain with the practice, not the individual clinician. A returning patient will continue receiving care from the practice, though treated by a different provider. The relationship between IDNs and organizations/facilities underneath will be a critical component to "get right."

The practice should be the primary entity in the directory, with providers listed as attributes under it. Practice administration and the management of provider details are likely handled by administrative staff at the practice level. As ASTP/ONC updates CEHRT, we recommend including directory API testing to ensure consistent directory operation within the practice's workflow and primary productivity tools. We recognize that ASTP/ONC and CMS will need to create incentives for all players to be responsible for updating and maintaining an accurate directory. Historically, such incentives have often been one-sided; sometimes placing the burden on the health IT vendor, the provider, or the payer. For the national provider directory to work, there needs to be incentives for all of the key stakeholders because each holds an important piece of the puzzle that one alone cannot solve independently.

2. Digital Identity

TD-3. Regarding digital identity implementation:

a. What are the challenges and benefits?

b. How would requiring digital identity credentials (for example, CLEAR, Login.gov, ID.me, other NIST 800-63-3 IAL2/AAL2 CSPs) impact cybersecurity and data exchange?

c. What impact would mandatory use of the OpenID Connect identity protocol have?

Identity and trust are closely related. Better identification and validation of individual providers, along with identification and validation of practice-level attributes, will enhance coordination of care across providers and other entities such as patients, payers, and public health organizations. That said, it is important that we also consider the patient, how they are identified, and how we match them across practices. Without consistency, it will continue to be challenging to scale individual access across networks.

The requirement to use OpenID Connect warrants further discussion, with regard to which components would be required versus optional. Although one strong ID used across multiple applications has its benefits, potential issues exist. Some individuals prefer diversifying their authentication methods to avoid a single point of failure for access to digital systems, applications, and assets. Moreover, a significant portion of the data access problem stems from locating data and overcoming obstacles rather than from authentication itself. Shifting the focus from mandatory use to supporting OpenID Connect might be more suitable, allowing users and patients to choose whether to consolidate or distribute their logins or to use a combination of both. The use of OIDC to create a credential with a Credential Service Provider (i.e., CLEAR, ID.me) within a single application, and then leveraging that credential (ID) to generate a token for the purpose of enabling patient access to their own data could be considered. It's the use of an existing standard to form a JSON Web Token (JWT) to increase trust, but it's only effective if the data holders agree to the use of the standard. Otherwise, it's wasteful to require and build if data holders won't respond.

It is also important to distinguish between the level of assurance that confirms identity (IALx) and the level of assurance that verifies appropriate credentials for accessing a resource (AALx) and the technology requirements for each. A resource can have a low IAL and high AAL—such as an email account secured with multi-factor authentication, which secures the account but does not verify the identity behind it. Numerous OpenID solutions do not perform identity verification, raising questions about whether requiring OIDC aims to improve AAL standards or facilitate IAS at scale. If the latter is the case, further discussions on demographics-based matching, risk management, and special effort means in context of an IAS. Specifically for IAS, if OIDC is used to create a credential that is re-usable by the consumer within their application of choice, it can be an effective way of ensuring that the identity confirmation part is well maintained. If OIDC is required to be shared across multiple systems, that adds a layer of complexity and risk that the industry is not yet ready to tackle.

The more important question to ask is – should IAL2 verification be required – and to that, we say yes. A person's identity should be required for their ability to access their

own clinical data. We believe that this is a more secure model because simply relying on a patient's portal credentials can be easily misplaced, lost, or stolen..

3. Technical Standards and Certification

TD-4. How can CMS better encourage use of open, standards-based, publicly available APIs over proprietary APIs?

While proprietary APIs will always exist, we endorse standards-based public APIs. CMS can support this by actively participating and providing its own APIs, facilitating a national provider directory starting at the organization level where API access resides. Including API endpoints in this directory would simplify access. However, simply listing an endpoint doesn't ensure easy connectivity. Although CEHRT mandates vendor-provided APIs, many aren't functional. The directory should validate API functionality regularly. We suggest a System Admin requirement for ASTP/ONC to periodically test API endpoints. Also, consider extended non-responsiveness without resolution as potential information blocking.

At the June 3rd listening session, there was significant discussion about shifting CEHRT towards testing APIs at the edge, rather than focusing on core functionality. This approach could standardize vital APIs and data access for both clinical and administrative purposes, while giving vendors room to innovate at the workflow level. We believe that this would be a good step in the right direction to help enforce successful interoperability.

TD-5. How could a nationwide provider directory of FHIR endpoints improve access to health information for patients, providers, and payers? Who should publish such a directory, and should users bear a cost?

It is advisable to avoid restricting the linkage of a directory solely to FHIR endpoints. Instead, it would be beneficial to support a broader range of interoperability endpoints, which could include IHE endpoints, Direct addresses, and other elements. Providers could also indicate which national or regional/state networks they participate in, to further show the available options. While there are positive developments towards using FHIR to replace legacy exchange methods such as document-based exchange under IHE standards, it is important not to abruptly discontinue technologies that continue to work effectively. Document-based exchange is expected to remain in place for many years to come. Transitioning from older technologies to newer ones takes time and effort, and there is often an overlap during the transition period.

As mentioned above, all key stakeholders to the directory should play a role in maintaining it, keeping it updated and accurate. Provider organizations play a role, their technology partners play a role, and payers play a role. We encourage ASTP and CMS to incentivize all key parties.

TD-6. What unique interoperability functions does TEFCA perform?

a. What existing alternatives should be considered?

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

Firstly, it is essential to consider not only the technological aspects of TEFCA but also its common agreement and governance. A robust framework is critical for connecting disparate networks with a common technical and policy ground. CommonWell has

emphasized that the key difference between Carequality and TEFCA is the presence of an unbiased authority—ASTP/ONC—which does not have commercial interests in the community's decisions. This neutral arbiter helps resolve disagreements among competitive entities, ensuring smoother operations.

Secondarily, data exchange benefits when various networks can interconnect. We saw this in practice in 2019 when CommonWell and Carequality connected to each other and began exchanging data. A chart of health data exchange over time showed a true hockey stick shaped leap that year. Since then, we have steadily seen increased levels of adoption and usage, but no jump was as proportionally as big of an impact as that first year.

Reverting solely to Carequality is not a viable solution. Although Carequality has served an important purpose, its issues with trust, policy, and technology have hindered its long-term potential. While there are several technical advantages of TEFCA over Carequality, the governance structure, particularly HHS's role, is a major strength of TEFCA.

A practical example illustrates this point: consider the vetting process for verifying a participating entity represents an actual provider. There was a practice, that was primarily digital and telehealth-focused, with a mission to serve communities with unstable primary care relationships This practice onboarded to Carequality but faced resistance from a significant implementer, preventing them from exchanging information under Treatment provisions.

Carequality and other frameworks require adherence to Applicable Law. Under HIPAA, covered entities must respond to data requests intended for patient treatment, but they also have the right to verify the requesting provider's legitimacy. Carequality does not itself vet provider entries; instead, it allows entities to apply their own business rules to determine if a requesting entity qualifies as a provider, creating scalability issues and potential conflicts. Without a resolution mechanism, one entity may refuse to exchange data with another even when there is substantial evidence of the requesting party’s validity.

Conversely, under TEFCA, if an implementer (now a QHIN) objects to an entity exchanging data freely under Treatment, the issue can escalate to the ASTP/ONC, if no consensus is reached among QHINs. This process ensures an impartial decision, unlike Carequality, which enhances governance and trust. Most entities clear the vetting process smoothly; only this one instance above has been escalated to the ASTP/ONC so far. This structured approach facilitates scale and resolution, reinforcing our belief that TEFCA, supported by HHS, is crucial for nationwide interoperability.

To further integrate organizations into TEFCA, improvements in the vetting process are needed. We firmly believe that the involvement of an impartial authority is vital for efficient and effective progression, preventing data gaps that could adversely affect patient care. Without improvements to vetting, many entities will be left out of exchange and without an adult in the room, some current QHINs and Participants may purposefully or inadvertently resist change.

Other issues that require attention exist in TEFCA today. The original design for the technical framework included QHINs with record location services (RLS) to enable comprehensive patient record searches within and across all networks. In the late stages

of development of the QTF (QHIN Technical Framework), requiring population level RLS capabilities was replaced with a requirement for RLS-like capabilities. This change has led to significant trust issues because it is unclear how a QHIN locates data within their network. Some QHINs take full responsibility for the patient population in their network with an MPI to match across entities, others forward patient discover requests to all entities in their network and aggregate the response and others selectively fan in based on criteria centered around geolocation – e.g. search the providers near a patient's home address(es). In fact, other methods could be used that were not listed here - the QTF has no standard for comprehensive search. Those outside of the immediate QHIN/TEFCA community did not understand that this requirement went away and were very surprised to hear that QHINs are not required to have a comprehensive RLS. The original concept of a "single on ramp" is diminished without this requirement.

With this, when a querying QHIN gets a "no patient found" response from a responding QHIN, the requestor has no idea where the responding QHIN looked. Did all entities in their QHIN say no? Or did 90% of them time out and never respond, and the 10% said no patient was found? The band-aid is to enable direct entity search capabilities within the framework as opposed to development of standard search methods, service level agreements and more informative responses that indicate comprehensiveness.

Likewise, the QTF did not set performance standards or service level agreements (SLAs). Setting SLAs was intentionally tabled until we had more exchange. We need to revisit these problems with an adult in the room to help set expectations and resolve what we cannot conclude on our own as competitive entities with natural self-interests at play. For all these reasons, TEFCA is much more than a technical standard and we encourage future, direct governance and support from HHS.

TD-7. To what degree has USCDI improved interoperability and exchange and what are its limitations?

a. Does it contain the full extent of data elements you need?

b. If not, is it because of limitations in the definition of the USCDI format or the way it is utilized?

c. If so, would adding more data elements to USCDI add value or create scoping challenges? How could such challenges be addressed?

d. Given improvements in language models, would you prefer a non-proprietary but less structured format that might improve data coverage even if it requires more processing by the receiver?

Medicine blends structured data with the need for free-form analysis. While language models can interpret unique document additions beyond USCDI, they have limitations and may not keep pace with medical advancements. We believe it is important to maintain and evolve USCDI to incorporate increasingly prevalent data elements but allow for a mechanism to exchange newer elements as they emerge before they are standardized.

TD-8. What are the most effective certification criteria and standards under the ONC Health IT Certification Program?

No comment from CommonWell.

TD-9. Regarding certification of health IT:

a. What are the benefits of redefining certification to prioritize API-enabled capabilities over software functionality?

b. What would be the drawbacks?

c. How could ASTP/ONC revise health IT certification criteria to require APIs to consistently support exchanging data from all aspects of the patient's chart (for example, faxed records, free text, discrete data)?

d. What policy changes could CMS make so providers are motivated to respond to API-based data requests with best possible coverage and quality of data?

e. How could EHRs capable of bulk data transfer be used to reduce the burden on providers for reporting quality performance data to CMS? What capabilities are needed to show benefit? What concerns are there with this approach?

We support certifying the interoperable edge of products, allowing tech companies to focus on workflows and product differentiation for current and future customers. Market needs can outpace regulation, causing vendors to lose technology cycles while complying with regulatory requirements.

The only drawback is that it may become harder to compare EHRs, leading to more time spent on product selection and implementation, but we believe the tradeoff is worth it.

API testing should include security and privacy compliance validation to ensure data movement is intentional and protected against infiltration by bad actors.

TD-10. For EHR and other developers subject to the ONC Health IT Certification Program, what further steps should ASTP/ONC consider to implement the 21st Century Cures Act's API condition of certification (42 U.S.C. 300jj-11(c)(5)(D)(iv)) that requires a developer's APIs to allow health information to be accessed, exchanged, and used without special effort, including providing access to all data elements of a patient's electronic health record to the extent permissible under applicable privacy laws?

Accessing patient data remains challenging despite low friction for provider-to-provider exchanges. The main issue is verifying that the requesting party is genuine and matches a record held by a responding provider. Enhancing identity standards can help confirm identities but doesn't ensure they match local records. To scale individual access safely, we need to move away from usernames and passwords to demographics-based matching, similar to provider data requests.

Individual Access Services (IAS) face two major concerns: safety and security. Missing data can lead to dangerous medical decisions, while mismatched records pose privacy risks. Using IAL2 for identity verification and standardizing a demographics-based

matching algorithm can address these issues. Providers currently use risk-based algorithms that match requests based on various demographics like name, address, phone number, date of birth, and email.

A national, standardized matching algorithm offers several benefits:

1. Increased trust through uniform algorithms that prevent blocking and false positives.
2. Reduced liability for responders, as strict algorithms provide defensible positions for rare false positives.
3. Easier resolution of non-matches, with clear guidance for patients on how to correct mismatched records.

Given addresses are great for disambiguating one person from another, but are prone to data entry errors, ASTP/ONC could do more to require address verification in the provider's electronic health record. Previously, the ASTP/ONC established a standard for how to document a patient's address, but it did not go so far as to require verification or validation. While 101 George Washington Hwy Apt 4, Jamestown, Massachusetts 34838 may be properly formatted with abbreviations approved by the Unites States Postal Service, it is possible that George Washington Hwy is officially Rt 9 and that 34838 is not a zip code in Jamestown at all. Digital verification of the individual's known address(es) in the IAL2 process is one solution, but IAL2 is not necessary for in person identity validation where a patient can present a proper ID. Using USPS APIs to verify addresses would be a great step forward to standardize address entry with the goal of better cross-system matching.

We encourage HHS to consider using deterministic identifiers for better patient matching. Payer IDs, social security numbers, and Medicare IDs can help match clinical records effectively. Issuing Medicare IDs before eligibility or creating a national health identifier could ensure better data completeness and continuity. Despite budget restrictions on a national health ID, early adoption of a Medicare ID, even voluntarily, could improve health decision-making.

TD-11. As of January 1, 2024, many health IT developers with products certified through the ONC Health IT Certification Program are required to include the capability to perform an electronic health information export or "EHI export" for a single patient as well as for patient populations (45 CFR 170.315(b)(10)). Such health IT developers are also required to publicly describe the format of the EHI export. Notably, how EHI export was accomplished was left entirely to the health IT developer. Now that this capability has been in production for over a year, CMS and ASTP/ONC seek input on the following:

a. Should this capability be revised to specify standardized API requirements for EHI export?

b. Are there specific workflow aspects that could be improved?

c. Should CMS consider policy changes to support this capability's use?

No Comment from CommonWell

4. Data Exchange

TD-12. Should CMS endorse non-CMS data sources and networks, and if so, what criteria or metrics should CMS consider?

Yes.

TD-13. What new opportunities and advancements could emerge with APIs providing access to the entirety of a patient's electronic health information (EHI)?

a. What are the primary obstacles to this?

b. What are the primary tradeoffs between USCDI and full EHI, especially given more flexible data processing capabilities today?

Working with structured datasets like USCDI is more straightforward, but language models now simplify handling unstructured information too. While specific advances from broader datasets are uncertain, enabling EHI through APIs widely is logical. Requestors who cannot work with the less standardized data can simply skip over the content and work with what they can until their capabilities advance.

TD-14. Regarding networks' use of FHIR APIs:

a. How many endpoints is your network connected to for patient data sharing? What types, categories, geographies of endpoints do you cover? Are they searchable by National Provider Identifier (NPI) or organizational ID?

b. How are these connections established (for example, FHIR (g)(10) endpoints, TEFCA/Integrating the Health Enterprise (IHE) XCA, or proprietary APIs)?

c. Do you interconnect with other networks? Under what frameworks (for example, TEFCA, private agreements)?

We connect with approximately 23,000 provider entities, including single site practices, large integrated delivery networks (IDNs) like the VA, and multi-site specialized practices such as Fresenius, which has thousands of sites. Our coverage is nationwide without specific areas of concentration. Currently, we exchange data using document-centric FHIR and IHE/XCA. Additionally, we are working towards network-wide broker-assisted FHIR within our community and have an active FHIR workgroup working on refining the standards and process for this transition within the year. We participate in Carequality as an implementer and in TEFCA as a Qualified Health Information Network (QHIN). As of today, we represent the largest number of active, legal entities in the TEFCA directory.

TD-15. Regarding bulk FHIR APIs:

a. How would increased use of bulk FHIR improve use cases and data flow?

b. What are the potential disadvantages of their use?

No comment from CommonWell

TD-16. What are the tradeoffs of maintaining point-to-point models vs. shared network infrastructure?

a. Do current rules encourage scalable network participation?

b. What changes would improve alignment (for example, API unification, reciprocal access)?

No comment from CommonWell

TD-17. Given operational costs, what role should CMS or ASTP/ONC or both have in ensuring viability of healthcare data sharing networks, including enough supply and demand, that results in usage and outcomes?

We do not think the viability of data sharing networks like CommonWell is at risk. We have been connecting the dots since 2013 and continue to see more Members and participation every day. That said, we are concerned about the viability of the frameworks that help bring networks like us together. With trust, operational and technical issues present in Carequality, we were expecting to move to TEFCA with a complete departure from Carequality in 2026. While we believe in our network and invite all to participate, we recognize some entities have different needs and strongly support a national framework that enables universal healthcare interoperability. We also feel TEFCA is unique due to its oversight and governance support at the federal level, and that industry alone would not function as well, particularly when a non-conflicted arbiter is needed, without federal support. We feel TEFCA is a very small investment for an outsized benefit.

5. Compliance

TD-18. Information blocking:

a. Could you, as a technology vendor, provide examples for the types of practices you have experienced that may constitute information blocking. Please include both situations of non-responsiveness as well as situations that may cause a failure or unusable response?

> We believe that provider organizations should have the ability to enable response to IAS queries. They should also be properly educated on the risk and benefits to individual patients and the healthcare ecosystem as they make the decision to participate or cite an exception to doing so. Unfortunately, we believe some vendors provide guidance to their customers that leans too heavily on risks, without a fair discussion of the benefits. Furthermore, we feel some vendors who appear to be capable of technology enhancements that could mitigate risk, do not ultimately develop these improvements.

b. What additional policies could ASTP/ONC and CMS implement to further discourage healthcare providers from engaging in information blocking practices?

> We do not think new policies are necessary, but do encourage use of existing policies with followup investigation into reported information blocking complaints while also looking for patterns of abuse. For example, while most complaints are filed against provider practices, are there concentrations of these complaints around specific EHRs or technologies used by these providers? Reported statistics indicate the actor type receiving the most official information blocking complaints is providers, but many patients are not aware of the technology products/companies in use by their providers nor whether the blocking activity is present across more implementations of the same technology and potentially not the provider's fault.

c. Are there specific categories of healthcare actors covered under the definition of information blocking in section 3022(a)(1) of the Public Health Service Act (PHSA) that lack information blocking disincentives?

> At our scale, it is hard to distinguish between blocking activity, technical issues and patient matching misalignment. The lack of standards for patient record matching makes this more difficult to troubleshoot. As stated earlier in this comment letter, we encourage a national matching standard to make this easier and to accelerate the adoption and utility of data from providers to patients.

TD-19. Regarding price transparency implementation:

a. What are current shortcomings in content, format, delivery, and timeliness?

b. Which workflows would benefit most from functional price transparency?

c. What improvements would be most valuable for patients, providers, or payers, including CMS?

d. What would further motivate solution development?

> No Comment from CommonWell