June 16, 2025
Submitted via: regulations.gov
Docket ID: CMS-2025-0087
File Code CMS-0042-NC
Submitted By: CareEvolution, LLC
Contact: policy@careevolution.com
Organization Type: Health IT Vendor

Comment on CMS RFI: Health Technology Ecosystem

CareEvolution appreciates the opportunity to respond to CMS's RFI titled "Health Technology Ecosystem". We are a health IT company committed to connecting healthcare to empower patients, caregivers, and researchers through modern, standards-based tools for secure health data access and exchange. Delivering safe, effective, and efficient care requires access to the longitudinal health history for a patient. Yet we are all aware that in our fragmented health care system, patient history is spread across a multitude of health plans, physician offices, urgent care centers, retail pharmacies, laboratory service providers, hospitals, social service and community service providers, and post-acute care facilities. The resulting information vacuum is a systemic weakness that compromises our best intentions and efforts to deliver optimal care. Across this country, health care professionals and patients alike face this reality every day. CareEvolution was born of this pervasive need to connect healthcare to enable patients to have access to their health record and clinicians to deliver efficient and effective care to the populations they serve. Our comments reflect our direct experience supporting patient-mediated access to thousands of payer and provider FHIR endpoints across the US, including Medicare APIs and certified EHR interfaces.

Since 2003, we have been at the forefront of the emerging and evolving "standards" for data interoperability and health information exchange inspired by the need to ensure that each and every one of us has a lifetime patient record at our fingertips. Starting in 2005 with the Markle Foundation and UK NHS Connecting for Health inspired efforts that culminated in the HITECH Act, we have been involved in operationalizing the efforts to connect our federated sprawling health system to better equip patients and caregivers with the longitudinal health, fitness, and environmental data that influences health outcomes and quality of life. Our technology stack and front line experience on the ground has evolved and grown with the maturing standards landscape from HL7 2.x broadcast to IHE query based exchange to Directed Exchange (secure messaging) to the more recent innovations with FHIR. Whether powering state health information exchange infrastructure (State Designated HIEs and RHIOs) or supporting DirectTrust certified secure messaging, or supporting CARES/CURES Act based Consumer Mediated Exchange, we have participated in the last 20 years of efforts in the Unites States supporting Medicare, Medicaid, CHIPRA, and Commercial plan members across the continuum of care.

Our on-the-ground experience aggregating and managing data on over 250 million US consumers for the largest health plans, integrated delivery networks, public health initiatives, public and private research organizations across the myriad of evolving standards provides us with a deeply pragmatic understanding of the current moment facing the healthcare information technology landscape. Having run some of the nation’s largest health information exchanges, aggregated data on behalf of the biggest IDNs and health plans, supporting the public sector agencies like CDC and NIH in some of their most ambitious longitudinal initiatives, we share our pragmatic perspective as follows.

We applaud CMS for this exceptionally well thought out (deep and broad) RFI. While we have views on a vast range (nearly all) topics of the RFI, we offer our perspective on the areas where we think it is most differentiated and pragmatic. These are organized per the RFI in the following areas:

TD - 3 Regarding digital identity implementation:

TD - 3 a. What are the challenges and benefits?

Multi-factor, high-assurance log-ins undeniably cut account-take-over fraud and make delegated data exchange more trustworthy, yet they also introduce the single biggest source of user friction: every extra selfie/driver-license scan knocks a share of seniors, rural patients, non-English speakers and privacy-conscious consumers out of the digital channel.

Under HIPAA, today a provider may release information to a person who is simply “known to the provider” (§ 164.514 h); most patient portals satisfy that with an in-clinic ID check plus username-password-MFA (i.e., AAL2 but only “IAL1.5” proofing). That pragmatic bar already supports tens of millions of Right-of-Access transactions per year, so the benefit of jumping to blanket NIST 800-63-3 IAL2 must be weighed against re-verifying 150 million existing portal users and retrofitting every payer site.

We believe that the current TEFCA requirements requiring IAL2 credentials regardless of whether a consumer already has a patient portal account setup (which requires each provider to have somehow validated the identity of the individual) is laudable but impractical. CMS should consider “grandfathering” any individual who already has a patient or member portal access to their EHR data at a Covered Entity.

TD - 3 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?

If CMS were to require Login.gov, ID.me, CLEAR, etc. for all API calls, cybersecurity would improve and record matching would be easier, but at a steep price: 1) 15-20% of Medicare beneficiaries have neither a smartphone nor broadband for remote proofing; 2) commercial CSP queues and fees could delay access; and 3) TEFCA’s Individual Access Services (IAS) would stall, because the Common Agreement and SOPs hard-code CSP-issued IAL2/AAL2 tokens - no CSP token, no query.

A middle path keeps the fraud controls without the enrollment cliff: 1) Continue to honor “known-to-provider + AAL2” for read-only API calls and patient-initiated sharing, but require IAL2 before higher-risk access such as bulk export. 2) Permit providers (or their portal vendor) to complete an IAL2 document check in-house and mint a cryptographically signed, portable credential. That satisfies NIST while removing dependence on a pre-approved third-party CSP.

The adage “enemy of good is better” comes to mind. The current TEFCA policy is admirable but comes at a massive cost. By honoring and building on the current “known to provider” model inherent in how Covered Entities manage consumer access to their health information, CMS could make the existing standard more pragmatic and support consumer needs.

TD - 3 c. What impact would mandatory use of the OpenID Connect identity protocol have?

OIDC is already the backbone for SMART-on-FHIR authentication, but making it explicit across all CMS/ONC-regulated APIs still matters: the protocol carries an acr / vtr claim that tells relying parties exactly which assurance tier was used, enabling the tiered model above. With the coming OpenID-Connect Federation 1.0 spec, a patient could “bring” any trusted credential - Login.gov, a state DMV wallet, even a FIDO passkey issued by her bank - and a payer or provider could trust it on first use. That both lowers barriers and distributes revocation/liability: if a credential is compromised, the issuer rotates keys once and every downstream relying party immediately rejects the token.

Agency action: 1) Set a two-level floor: Codify “known-to-provider + AAL2” as the minimum for patient-facing read access while designating full NIST IAL2 only for higher-risk workflows. 2) Amend TEFCA SOPs to allow IAS transactions at the baseline level or accept provider-performed IAL2 proofing, so CSP dependence does not bottleneck nationwide roll-out. 3) Mandate OIDC (+ FAPI/UDAP) federation claims in every certified API endpoint so any credential carrying the required assurance automatically interoperates - no special effort, no wholesale re-credentialing.

We believe the current approach is laudable but far too technocratic and misses the real world needs of U.S. Consumers.

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

Today an app developer must negotiate a patchwork of registration portals: one global form for most Epic or Cerner sites, but hundreds of one-off, often-broken web forms for payers and many smaller EHRs. That fragmentation - not the FHIR spec itself - is now the single biggest “special-effort” hurdle for third-party innovators.

CMS can eliminate that friction by standing up a national Dynamic-Client Registration hub that mirrors the model already proven in UK/EU open banking: An app developer would authenticate to the hub with a certificate that proves it is a legitimate HIPAA Business Associate or consumer app (just as a bank-regulated TPP must hold an FCA/PSD2 certificate). The hub would issue a UDAP-conformant software-statement that packages the app’s metadata - name, logo, redirect URIs, JWKS URL, requested scopes - and is cryptographically bound to the developer’s certificate. Any provider or payer authorization-server need only accept that signed JWT during the first OAuth interaction; the server can auto-provision a client-ID with no manual ticket, and revoke it automatically if CMS suspends the certificate. Epic, Cerner, Athena, and some other EHR customers already benefit from a similar global-registration feed; extending the same convenience to Medicare Advantage plans, Medicaid MCOs and commercial payers would remove weeks of queue time from every new integration. Patients continue to use the portal credentials they already have; the strong assurance lives in the certificate and the hub’s vetting process, so CMS does not have to impose IAL2 credentials on end-users for this use case.

Open banking has shown that a certificate-backed software-statement plus dynamic registration can scale to thousands of banks and millions of consumers while keeping onboarding essentially zero-touch. CMS can reuse the UDAP Dynamic Client Registration profile (already referenced in TEFCA) and require certified Health IT modules to consume a CMS-signed software-statement as a condition of the “Standardized API” criterion. That single step would replace hundreds of brittle spreadsheets, e-mail threads and support tickets with an instant, machine-readable handshake - precisely the kind of no-special-effort ecosystem Congress envisioned.

Agency Action: Create a CMS-hosted UDAP/Dynamic-Client Registration service that issues signed software-statement JWTs; update ONC certification and PI/MAPD contract language to require provider and payer authorization servers to auto-import those statements at first contact, retiring bespoke registration portals and putting payers on equal footing with EHR vendors.

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?

A single, authoritative directory of every provider’s and payer’s FHIR endpoint would transform today’s scavenger-hunt for connection details into a simple look-up, eliminating one of the most stubborn obstacles to seamless data exchange. With an easy-to-query registry, software could resolve “Dr. Nguyen (NPI 1234567890)” to “https://ehr.acmeclinic.org/fhir/R4” instantly, collapsing a process that now takes phone calls, web searches, and spreadsheet maintenance into a sub-second query. This lowers integration costs for small practices and start-ups, makes nationwide roll-outs economically feasible, and - by putting independent and rural sites in the same directory as large health systems - promotes equitable access to data exchange.

Because such a directory is public-interest infrastructure, stewardship should rest with HHS - specifically ONC and CMS - whose authority over interoperability policy and existing National Provider Directory and Lantern endpoint-scanner initiatives give them both the mandate and a technical head-start. Maintaining the directory as a free (or nominal-cost for high-volume commercial queries) public resource replicates the GPS and NPI models that have powered decades of innovation; the modest hosting and verification costs should be treated as part of federal interoperability funding.

Technically, the directory should publish entries in the HL7 FHIR Endpoint and FAST Directory profiles and expose both real-time REST queries and nightly bulk-download files. Records must be indexed on multiple keys - NPI, CCN, organization OID, taxonomy, and geography - so that apps, clearinghouses, and HIEs can find the right endpoint no matter which identifier they start with. Updates should be tied to existing CMS program touchpoints such as Medicare enrollment renewal, MA contract renewal, or Promoting Interoperability attestations, ensuring that endpoints stay accurate without adding a new reporting burden. To bridge document- and API-based exchange, each listing should also surface the organization's TEFCA QHIN affiliation and any XCPD service addresses.

Agency Action: CMS and ONC should extend the National Directory work to include mandatory, brands-and-endpoints listings for both providers and payers; require participants to refresh their records as part of routine enrollment or PI attestations; and publish the aggregate directory free of charge via REST and bulk files, making it the authoritative mechanism for discovering exchange partners nationwide.

TD - 6 What unique interoperability functions does TEFCA perform?

From our point of view, TEFCA's unique value is not its technical standard (i.e. SOAP/XCA plumbing) - it is the federal trust fabric wrapped around that technical plumbing. The Common Agreement supplies 1) a single, nationwide liability framework that lets a QHIN rely on another QHIN's identity-proofing without separate contracts; 2) a mandatory Record Locator Service (RLS) so one query can discover records held by every other QHIN; and 3) an explicit right for patients (Individual Access Services) to use those same pipes. No other programme combines all three at national scale, and Medicare, VA, DoD, and six commercial QHINs have already invested heavily in onboarding to that fabric.

TD - 6 a. What existing alternatives should be considered?

For pure transport we already have mature, simpler tools: plain-HTTPS FHIR APIs secured with OAuth 2.0/UDAP, the HL7 FAST security and identity guides, and the emerging National Endpoint Directory. Point-to-point FHIR, however, still lacks a shared liability contract and a standard for cross-network patient matching. We therefore recommend a modular accelerated evolution, not abandonment, of TEFCA: direct the RCE to pilot native QHIN-to-QHIN FHIR over HTTPS by 2027 and to allow directory-driven IAS queries that target only the QHINs a patient selects. The **trust agreement** stays intact, yet low-risk, patient-directed pulls bypass the heavy RLS broadcast and avoid another complex channel.

TD - 6 b. Are there redundant standards, protocols or channels or both that should be consolidated?

Running both XCA/SOAP and FHIR inside every QHIN is wasteful. Once the native-FHIR lane is proven, CMS should authorise QHINs to retire SOAP for IAS traffic and eventually for provider queries. At the same time, CMS and ONC should merge duplicative endpoint lists (RCE’s RLS, NPPES “FHIR” fields, and FAST/Lantern data) into one public, FHIR-queryable directory. Consolidating on a single transport (FHIR/HTTPS) and a single directory eliminates the need for parallel Carequality gateways, separate DirectTrust certificates, and other bespoke bridges.

Agency Action: We recommend CMS instruct the RCE to add a “Module C” to TEFCA: native QHIN-level FHIR with OAuth 2.0/UDAP security and optional directory-targeted IAS queries, coupled with a roadmap to sunset SOAP/XCA once all QHINs pass a conformance test suite.

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

USCDI has unquestionably raised the baseline: since v1 became part of ONC certification in 2020, every certified EHR can emit the same coded meds, labs, vitals, allergies, immunizations, demographics and notes, which in turn jump-started SMART-on-FHIR apps and reduced the need for one-off interfaces.

That said, three realities limit its practical impact:

1) Several high-value domains are still only partly covered. Advance directives, for example, do appear - but only in draft USCDI v5, which is not yet tied to certification, so few vendors expose the element in production APIs. Radiology references (ImagingStudy/DICOM) were added in v3 and refined in v4, yet many health systems still suppress them because their picture-archiving system sits outside the core EHR. Social-determinants observations were added in v3, but vague value-set guidance and immature mappings keep them from flowing widely.
2) Data holders treat USCDI as a ceiling, not a floor. The moment an element is absent from the enumerated list, many providers and payers simply omit it - even when the Cures Act’s “all EHI” clause allows, and patients expect, broader sharing.
3) Certification tests stop where the spec stops. If Inferno doesn’t test it, vendors rarely ship it; thus the problem is less about the format and more about utilization pressure.

TD - 7 a.Does it contain the full extent of data elements you need?

No. Even at v5, gaps remain: high-fidelity images and waveforms (e.g., echocardiogram loops, EEG strips); medication-administration details (actual doses, not just orders); granular genomics and oncology staging; and continuous device or remote-monitoring feeds such as CGM data.

TD - 7 b. If not, is it because of limitations in the definition of the USCDI format or the way it is utilized?

Mostly use and adoption. The specification already allows richer content through extensions, but vendors halt at what is explicitly required for certification; hence good data are left behind because they are not tested or incentivized.

TD - 7 c. If so, would adding more data elements to USCDI add value or create scoping challenges? How could such challenges be addressed?

Carefully phased expansion would close dangerous blind spots. The key is to release each new class with clear value sets, a US Core profile, and an Inferno test script before the compliance clock starts, so implementers build once instead of revisiting mid-cycle.

TD - 7 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?

Yes - pair the structured USCDI core with required sharing of accompanying narrative or binary artifacts (notes, PDFs, DICOM) so AI tools can mine unstructured context the sender did not code. Waiting for perfection in discrete fields leaves valuable signal trapped.

Agency Action 1) End the ceiling effect: In both certification and Promoting Interoperability scoring, award full credit only when all requested EHI - not just USCDI - is returned to the patient or authorized app. 2) Adopt a gradual version cadence. Move certification from USCDI v1 to v3 in the next cycle, then to v5 two years later, but back-port v5's new classes as "R4++" US Core extensions. This avoids a premature, dual-stack FHIR R6 mandate that would saddle vendors with years of parallel maintenance for marginal benefit. 3) Test what you require. Publish Inferno test decks and sample payloads for every new USCDI element before the enforcement date so vendors can code once and be done. 4) Clarify that narrative counts. Update information-blocking guidance: withholding unstructured documents because they are "outside USCDI" violates the "all EHI" rule. By reinforcing that USCDI is the floor, not the ceiling, and by expanding it pragmatically while mandating transmission of the surrounding narrative, CMS and ONC can convert paper progress into data that patients, payers and apps actually see.

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

The clear game-changer is §170.315 (g)(10) - the SMART-on-FHIR R4 API mandate. By standardizing OAuth, scopes, and resource schemas, it let any conformant app run on every certified EHR. Results speak for themselves: 400+ third-party apps now live on SMART; tens of millions of patients pull records into Apple Health and other tools; startups integrate with all major EHRs in weeks, not months.

Classic criteria - SCRIPT e-prescribing, C-CDA exchange, SNOMED/RxNorm/LOINC - still matter, but their reach is amplified precisely because they ride over the FHIR gateway.

Agency action: 1) Protect the API core. Keep (g)(10) as the anchor; add Bulk FHIR and writes, but resist drifting back to UI-feature checklists. 2) Reuse the same stack everywhere. New mandates for prior auth, price transparency, quality, and EHI export should piggy-back on SMART/FHIR security and transport. 3) No rushed FHIR R6. Extend "R4 ++" first; require R6 only when tooling and clear ROI arrive, avoiding a costly dual-version gap.

Doubling-down on an API-centric, SMART-on-FHIR foundation keeps innovation plug-and-play and patients in control of a vibrant app ecosystem.

TD - 9 Regarding certification of health IT:

TD - 9 a.What are the benefits of redefining certification to prioritize API-enabled capabilities over software functionality?

Modularity & competition: an EHR that exposes complete, well-profiled APIs lets providers bolt on best-of-breed modules instead of waiting for monolithic road-maps. Future-proofing: once all data are accessible via transport-agnostic APIs, upgrades (e.g., AI notation services, remote monitoring feeds) plug in without new regulation.

TD - 9 b. What would be the drawbacks?

There are some very specific drawbacks to an early pivot FHIR R6. The single biggest risk of moving the certification baseline from R4 to R6 in the next cycle is massive churn with negligible clinical upside:

Because the new spec sits at a new base URL (e.g., /fhir/R6), every OAuth registration, refresh-token, and "remember-me" session issued to the 300-plus SMART-on-FHIR and Blue-Button apps in production today would immediately fail. Millions of seniors would have to reopen each app, re-authenticate, and re-authorize data sharing - a usability hit that we know from experience will drive significant abandonment.

The only way to avoid that user-level breakage is for vendors to stand up two fully supported endpoints - R4 for legacy traffic and R6 for new traffic - for at least two years. That doubles security patching, change-control, performance testing, and certification overhead precisely when small practices are already struggling to keep their portals afloat.

For the workflows that dominate real-world exchange - USCDI-level read/write, $export for quality, provider-payer prior-auth - R4 already works. The marquee R6 gains (improved Subscriptions, canonical grammars, partitioned bulk export) can be back-ported as extensions without forcing a wholesale version jump.

Vendors have just finished their R4 Inferno testing. Re-tooling for R6 within a year or two means new interface-spec work, new test scripts, and another round of ONC real-world testing - not to mention retooling every third-party app.

Agency Action: We recommend a pragmatic alternative: “R4 ++” freeze-and-extend

1) Freeze certification on R4 through 2027. Lock the base spec so implementers get a predictable runway to mature existing APIs. 2) Back-port the few must-have R6 capabilities - SubscriptionTopic, canonical-URL fixes, and partitioned bulk export - as official R4 extensions profiled in a US Core addendum. 3) Stand-up a “business-value workgroup” in 2026. Let payers, providers, app developers, and patient advocates quantify whether the remaining R6 deltas justify a full bump. 4) If R6 adoption proceeds, require a 24-month “graceful-upgrade” window in which servers must support transparent content negotiation (R4 and R6 at the same base URL) and an Inferno dual-mode test harness - so implementers migrate once and patients never lose token continuity.

This “R4 ++” approach avoids a costly dual-version purgatory, shields patients from broken app connections, and still lets innovators pilot the handful of truly useful R6 features immediately via extensions.

TD - 9 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)?

Certification test overhaul: add a “Whole-Chart Export & Query” criterion that 1) exercises FHIR R4 endpoints for every resource the system stores (including Binary for scans, DocumentReference for external PDFs, and Provenance) and 2) runs an Inferno-style test harness against a reference account containing scanned faxes, imaging links, narrative notes, SDOH assessments and device waveforms. Passing = 100 % retrieval.

TD - 9 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?

Promoting Interoperability rewrite: award PI points only when providers demonstrate automated, timely fulfilment (>95% within 24h) of patient- and app-initiated FHIR pulls including attachments. Non-fulfilment counts as information blocking. Publish quarterly “API responsiveness” dashboards.

TD-18. Information blocking:

TD - 18 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?

In the routine course of supporting patient-mediated exchange, we connect to thousands of provider, payer, and federal FHIR endpoints and have documented a recurring pattern of obstacles that unreasonably interfere with data access.

First, several EHR vendors erect procedural barriers: for example, a hospital will not enable the same certified FHIR endpoint we already use elsewhere until each facility grants one-off approval, while another vendor portal frequently malfunctions, preventing us from even filing the enablement ticket. Both delays keep patients from accessing data that is already required to flow “without special effort.”

Second, many payer Patient-Access APIs fail basic conformance. Common defects include misconfigured OAuth scopes, missing capability statements, and incomplete US Core resources. Some health plans refuse to issue production credentials until a third-party app signs proprietary legal terms or agrees to traffic caps well below CMS guidance, effectively discouraging routine patient use.

Finally, the Department of Veterans Affairs imposes burdens far beyond typical HIPAA or ONC (or GDPR) practice: multiple rounds of privacy-policy rewrites, mandated grade-12 readability, broad data-deletion commitments, and a 60-request-per-minute rate limit that makes it impractical to retrieve a complete veteran record. These hurdles collectively delay or deter Veteran-directed access and appear misaligned with the Cures Act’s prohibition on unreasonable interference.

TD - 18 b. What additional policies could ASTP/ONC and CMS implement to further discourage healthcare providers from engaging in information blocking practices?

CMS and ONC can counter these practices by publishing a public “endpoint scorecard” that displays uptime, SMART launch success, and resource completeness for every certified product and regulated payer. A thirty-day cure clock tied to Promoting Interoperability points (for providers) or civil monetary penalties (for payers) would give actors a clear timeline to fix defects. In addition, certification should require self-service dynamic-client registration so third-party apps are not forced into months-long manual queues. Treating excessive throttling or policy hurdles, such as the VA’s broad contractual demands, as information blocking would further deter misuse.

TD - 18 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?

Today, small practices below the MIPS threshold and federal entities such as the VA face no monetary penalties for blocking behavior. CMS should coordinate with state licensing boards to extend professional-discipline risk to non-MIPS clinicians and work with OMB to apply equivalent disincentives to federal agencies. Closing these gaps will ensure that every data holder - large or small, public or private - has a tangible reason to eliminate unnecessary barriers to patient-directed exchange.