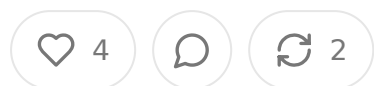


The Health Technology Ecosystem RFI An Incumbent-Centric Speculative Analysis on Strategic Positioning, Policy Shaping, and Market Realignment

MAY 14, 2025



Share

The Centers for Medicare & Medicaid Services' 2025 Request for Information on the Health Technology Ecosystem marks a subtle but decisive evolution in federal posture. It signals not only the maturation of CMS and ONC's interoperability agenda but also the intent to deepen government influence over the infrastructure innovation pathways of digital health products. What makes this RFI uniquely consequential is not its exhaustive list of questions, nor its novel policy anchors, but the rare clarity with which it invites the technology market into a dialogue about regulatory shaping. In so doing, it offers a thinly veiled message to incumbent technology vendors—particularly electronic health record (EHR) firms, health information networks, digital therapeutics developers, and payer-aligned IT infrastructure providers—that their participation in the transformation of the Medicare digital layer will not be optional. How these stakeholders choose to respond will determine whether they become architects or adversaries in this digital health renaissance.

Large EHR vendors, long criticized for interoperability foot-dragging, now find themselves in an uncomfortable dual role. On one hand, they are the necessary custodians of the structured data ecosystem. On the other, they are increasingly perceived as the bottlenecks preventing patient-directed data fluidity. The RFI explicitly calls for richer FHIR-based access, a more uniform patient experience across applications, and a reconfiguration of patient data rights that could, if fully realized, shatter long-standing proprietary architectures. The dominant vendors

this category—those whose revenue models rely on per-seat licensing, interface and cloud hosting contracts—will likely seek to blunt the force of these changes through carefully worded lobbying. Their strategy will revolve around emphasizing patient safety, cybersecurity risk, and data integrity as justifications for why open APIs cannot be made fully symmetrical with internal data flows. These vendors propose “graduated interoperability tiers,” arguing that only certain data elements should be made available to third-party apps due to clinical misinterpretation risk and liability exposure. In practice, this would preserve their strategic control of high-value data objects—clinical notes, diagnostic imaging metadata, structured genomics, social determinants of health annotations—even as they comply superficially with CMS demands.

A second axis of lobbying from these same EHR vendors will likely be directed toward CMS’s implication that future rulemaking may favor health IT products that meet broader certification thresholds, including TEFCA participation and full USCDM compliance. Incumbents will aim to convert these potential policy changes into market protection mechanisms. By encouraging CMS to tie digital health reimbursement or app eligibility to ONC-certified systems, incumbent EHR vendors can reduce the competitive threat from unregulated or semi-regulated app ecosystems that bypass traditional workflows. Rather than fight TEFCA or certification expectations directly, they will seek to embed their own API gateways and trust frameworks in the backbone of these initiatives. This would transform potential existential threats into rent-seeking opportunities.

Meanwhile, payer-aligned technology vendors—particularly those invested in claims data aggregation, prior authorization APIs, quality reporting engines, and risk adjustment platforms—will react to the RFI with a blend of opportunism and caution. For these firms, the proliferation of patient- and provider-facing APIs threatens to disintermediate their role as intermediaries. However, they may also see an opportunity to expand into adjacencies like real-time clinical decision support or utilization management via patient-facing applications. Their lobbying efforts will aim to convince CMS that clinical quality measurement and outcomes tracking should not be the responsibility of third-party apps but should instead be handled through

trusted payer pathways. They will advocate for CMS to fund infrastructure grant pilots that make use of payer-aligned data ecosystems as “regulatory scaffolding” for patient engagement efforts. This framing allows them to capture policy rents while avoiding exposure to more competitive, decentralized app marketplaces.

In contrast, emerging digital health product vendors, especially those building new apps for chronic disease management, remote monitoring, and patient navigation, are likely to welcome the RFI’s tone and scope. Yet they too face strategic dilemmas. On one hand, CMS’s explicit focus on promoting third-party app development, patient data portability, and value-based care alignment reads as a clear signal of future market expansion. On the other hand, the document’s subtext—particularly its references to certification, standardized APIs, and “provider-approved workflow”—hints at a regulatory regime that could replicate the high compliance costs and other restrictions that historically constrained innovation in the EHR space.

These vendors will likely adopt a two-pronged lobbying approach. First, they will petition CMS to develop a “lightweight certification” model that validates apps based on privacy, usability, and efficacy without requiring ONC-level formalism. This could take the form of a digital health formulary, akin to a Medicare Part D plan’s preferred drug list, allowing CMS to promote apps without declaring them as medically necessary or issuing coverage determinations. Second, they will push for reimbursement models that allow providers to prescribe or recommend digital tools without incurring financial or liability risk. These vendors will aim to shift the burden of proof for app efficacy away from randomized controlled trials and toward real-world evidence gathered through API-enabled usage data, a paradigm that would advantage software-first companies over traditional clinical service providers.

Parallel to these efforts, large national payers and managed care organizations will interpret the RFI through the lens of operational cost containment and competitive positioning. For these entities, digital health products are a strategic lever not only for member engagement but also for reshaping provider networks and accelerating the transition to risk-based contracting. However, they will be wary of any CMS initiative that forces them to relinquish control over digital identity frameworks, member data custodianship, or API gatekeeping. Their lobbying will focus on shaping the TEH

implementation in ways that preserve their position as adjudicators of data legitimacy. Expect calls for CMS to grant payers expanded authority to act as trusted data validators within national health information networks, essentially codifying their role as default consent brokers for patient data exchange.

Additionally, these payers will seek to avoid regulatory exposure for “information blocking” allegations that could arise from their increasingly sophisticated data monetization strategies. They may push for clearer safe harbor rules that allow data suppression under the guise of analytics pipeline optimization, citing cybersecurity and fraud prevention as justifications. At the same time, they will likely attempt to inject this language into future CMS guidance that affirms the right of managed care organizations to use AI-powered decision support tools—even when those tools operate on opaque logic or undisclosed risk stratification algorithms—as long as they meet performance benchmarks. This would allow them to maintain algorithmic opacity while complying technically with transparency mandates.

Telehealth and remote patient monitoring vendors occupy a more complex strategic niche. While the RFI appears to favor their long-term integration into Medicare workflows, it also presages new regulatory burdens. By emphasizing the need for digital health products to interoperate with FHIR endpoints, conform to identity and credentialing standards, and integrate with claims and encounter data streams, CMS is signaling an eventual convergence between app functionality and legacy health IT compliance paradigms. Telehealth platforms that once operated under emergency waivers or as consumer-grade utilities will be drawn into a new layer of regulatory scrutiny.

Their response will be to lobby for special carve-outs and exceptions based on care delivery modality. They will argue that synchronous video visits, asynchronous messaging, and RPM alert streams represent fundamentally different data artifacts than structured clinical data, and that imposing the same interoperability rules will stifle innovation. They may also advocate for CMS to classify them as “ancillary clinical infrastructure” rather than formal health IT vendors, thereby shielding them from TEFCA obligations or ONC certification criteria. This framing would allow

them to retain the technical agility needed to integrate with wearables, ambient sensors, and AI-based triage tools while minimizing compliance costs.

Simultaneously, these vendors will push for new reimbursement codes or quality adjustment factors that explicitly reward digital engagement. Their goal will be to transform utilization of their platforms into quantifiable value-based performance metrics, particularly in chronic disease cohorts. This requires aligning their internal data collection pipelines with CMS quality programs, a move that could open the door to real-time claims adjudication, value-based software formularies, or even performance-based payment models for digital therapeutics.

In the broader analytics and population health segment, vendors offering clinical decision support, predictive modeling, and AI-enhanced risk stratification will view the RFI as both a roadmap for product expansion and a regulatory hazard. These companies operate on the assumption that superior data liquidity translates into superior insights, which in turn can be monetized through B2B contracts with private health systems, and public health entities. However, the RFI's emphasis on transparency, algorithm accountability, and value-based outcome alignment could disrupt their current operating model, especially if CMS enforces auditability of clinical algorithms as a precondition for digital health integration.

Their strategic lobbying will concentrate on limiting the granularity of explainability requirements and pushing for voluntary, self-attested models of algorithm transparency. They will attempt to shape CMS guidance to define “transparency” in terms of intended use cases, training data provenance, or external validation reports rather than proprietary model weights or logic chains. They may even offer to develop industry-led accreditation frameworks for clinical AI systems, aiming to preempt government standard-setting with a more flexible, self-regulated regime.

At the same time, these analytics vendors will petition CMS to create a new class of digital quality metrics that rely on passively collected data from patient apps, remote monitors, and ambient sensors. Their ultimate goal is to institutionalize their platforms as the data layer beneath next-generation quality measurement programs. They will argue that only real-time, AI-driven models can fulfill the promise of

longitudinal risk prediction, population health optimization, and real-world out tracking across fragmented care settings.

Yet, these arguments will be met with skepticism from consumer privacy advocates and cybersecurity hawks who see the convergence of AI, patient data liquidity, and limited transparency as a recipe for exploitation. These countervailing forces will likely prompt CMS to balance permissiveness with audit readiness, potentially introducing algorithm disclosure thresholds or adverse event reporting mandates for software-driven care decisions.

Meanwhile, health information exchanges (HIEs) and private interoperability networks will find themselves on the defensive. Although the RFI acknowledges their role in facilitating patient access to data, it simultaneously questions the long-term necessity of centralized data intermediaries in a FHIR-native, TEFCA-enabled, patient-directed data flow architecture. HIEs whose business models depend on transaction fees or exclusive regional data aggregation contracts will view this RFI as a quiet declaration of obsolescence.

Their lobbying will take the form of institutional legitimacy assertion. They will argue that centralized entities remain critical for patient identity reconciliation, clinic context normalization, and adjudication of conflicting data elements. They may advocate for a regulatory requirement that all digital health products interface with at least one qualified HIE, effectively re-intermediating themselves into an otherwise disintermediated model. Expect calls for a new class of “Health Data Adjudication Networks,” staffed by credentialed informatics professionals and endowed with federal funding, as a strategy to reassert relevance.

Additionally, HIEs will likely partner with state Medicaid agencies and regional quality collaboratives to demonstrate their value in public health surveillance, especially in the context of health equity analytics and chronic condition mapping. These partnerships will form the rhetorical backbone of their defense: that without them, digital health ecosystems risk fragmenting into an uncoordinated patchwork of data silos once again.

Large platform technology vendors—those straddling the lines between infrastructure, analytics, and developer ecosystems—will treat this RFI as both opportunity and threat. Companies like Amazon, Google, and Microsoft, along with cloud-native healthcare platform players, have spent years laying the foundation for HIPAA-compliant data lakes, FHIR-native storage, and real-time analytics pipelines. For them, CMS’s interoperability mandates represent the critical scale enabler for health cloud adoption. If the government mandates data liquidity, someone must manage that data, and that someone will invariably be a hyperscale provider.

However, these firms are acutely aware that full participation in the healthcare infrastructure layer brings with it public scrutiny, political risk, and regulatory entanglement. Their lobbying will take the form of infrastructure altruism.

These startups often target the seams between EHR systems and patient experience layers, or between payer prior authorization workflows and provider-facing documentation burden. The RFI’s expansive scope and its implicit openness to new forms of digital engagement signal to these players that their products might finally find traction with Medicare beneficiaries and institutional buyers. However, they are also keenly aware that a sudden swing toward regulation-heavy, certification-centric governance could render their products non-viable, especially if they are forced to comply with security, identity, and interoperability standards designed for billion-dollar enterprises.

Their lobbying posture, though less resourced and more fragmented, will take shape through coalitions and trade groups advocating for sandbox programs, incremental compliance pathways, and pilot designations for digital health innovation. They argue that CMS should formally recognize and protect innovation-stage applications by creating “emerging digital health” exemptions or alternative certification pathways. Their aim is to avoid being regulated out of relevance by rules that were meant to bring stability to the market but risk entrenching existing power structures.

These firms will also urge CMS to define a new class of reimbursable services around digital navigation, algorithm-assisted engagement, and passive monitoring. Their lobbying language will emphasize patient empowerment, rural access, and behavior

health penetration, hoping to align their commercial needs with broader policy objectives around health equity and underserved populations. They will also lean heavily into real-world evidence collection, proposing that app telemetry and engagement metrics be used as proxies for efficacy, particularly in therapeutic areas where randomized controlled trials are unfeasible.

The RFI's specific inquiries around data accessibility and integration will have ripple effects across a different but increasingly central group of vendors: those specializing in clinical data transformation, data normalization, and semantic enrichment. These are the companies that build the infrastructure required to ingest HL7 v2 messages, free text clinical notes, and unstructured imaging metadata into FHIR-native endpoints that support analytics, interoperability, and patient-facing use. For them, the RFI represents validation of their relevance, but also a possible commoditization event.

Their lobbying efforts will center around making their function mandatory. They will urge CMS to mandate data quality minimums, semantic normalization thresholds, and metadata completeness audits for all data exposed via FHIR endpoints or Blue Button APIs. If successful, this would create a regulatory requirement that only they are currently equipped to fulfill, insulating their market position from low-cost entrants or in-house builds. They will also attempt to align with EHR vendors, offering themselves as partners in achieving regulatory compliance while privately positioning themselves as critical enablers of interoperability.

This group will also be the most vocal in opposing any CMS movement toward "lightweight" or consumer-grade interoperability. They will argue that patient empowerment and third-party app access are noble goals but must not come at the expense of clinical coherence, data integrity, or safety. Expect to see position papers from these vendors warning against a "data deluge" that could compromise clinical workflows unless appropriately filtered, structured, and interpreted. They may even call for the creation of a formal role—"data exchange quality assurance intermediary"—that would license and certify entities capable of converting raw data into FHIR-native, semantically complete datasets suitable for downstream use.

As for value-based care organizations, particularly ACOs and MSSP participants, RFI offers both the promise of greater data liquidity and the threat of added compliance complexity. Many of these organizations have spent years assembling fragmented data infrastructure, aligning provider incentives, and building bespoke analytics to meet quality measures and manage risk. The idea that CMS might not require them to adopt a new set of APIs, identity protocols, or interoperability frameworks to continue accessing performance incentives will be met with concern, not outright resistance.

Their lobbying will focus on creating carve-outs and grandfathering clauses. They will seek assurance that existing data aggregation workflows and payer-provider interactions will not be invalidated by new federal mandates. Simultaneously, they will advocate for VBC-specific standards, arguing that organizations already operating under shared risk contracts should be subject to different, more flexible interoperability requirements that prioritize clinical outcomes over strict data format compliance. This might include, for example, the use of patient-reported outcomes or community-based SDOH datasets as valid inputs into quality measurement, even if they fall outside the current USCDI schema.

In parallel, these groups will push for formal CMS recognition of digital tools as enablers. They will propose that APM participants receive bonus payments or risk adjustment credits for deploying validated digital therapeutics, remote monitoring tools, or AI-driven care coordination platforms. Their argument will hinge on the claim that digital tools reduce downstream costs and increase adherence, thus aligning with Medicare's broader cost-containment objectives.

Yet even among APMs, there will be divisions. Larger, better-capitalized entities that operate multiple MSSP tracks or run commercial VBC contracts alongside Medicare ones will likely favor more aggressive standardization. For them, every new interoperability requirement is another chance to consolidate their technical and clinical infrastructure advantage. Smaller or rural ACOs, by contrast, will seek exemptions, phased timelines, or alternative reporting mechanisms to avoid being crushed under the weight of simultaneous IT modernization and clinical transformation.

Another crucial axis of response will come from the privacy and civil liberties community. While these organizations are not commercial vendors, their influence on policymaking, especially in the realm of digital identity and data governance, is profound. The RFI's emphasis on trusted identity credentials, digital signatures, centralized patient access mechanisms will trigger concern about surveillance, de-re-identification, and potential misuse of health information under the guise of innovation.

These groups will not lobby in the traditional sense but will organize public comment campaigns, publish critiques, and push for formal oversight mechanisms. They will urge CMS to impose strict data minimization principles, consent renewal requirements, and independent auditing of any digital health platform that touches sensitive beneficiary data. Expect proposals for patient data dashboards, algorithm transparency panels, and opt-out registries for any platform interfacing with CMS APIs.

From a political economy perspective, their influence could derail or significantly delay the implementation of the most ambitious elements in the RFI, particularly those that envision continuous, bidirectional data flows between CMS infrastructure and third-party platforms. If these privacy watchdogs gain traction, CMS may be forced to incorporate stronger governance provisions, clearer patient rights statements, and multi-stakeholder oversight bodies into any future rulemaking.

At a meta-level, the collective lobbying posture of the health tech ecosystem will manifest as a conflict between two temporal visions of digital health. One vision, advanced by legacy vendors and institutional actors, imagines digital health as an extension of existing clinical workflows: something to be normalized, credentialled, and appended to brick-and-mortar medicine. The other, championed by startups, patient advocates, and consumer tech platforms, sees digital health as a parallel modality: asynchronous, decentralized, and self-directed.

The RFI, perhaps unintentionally, invites both visions to compete for federal blessing. It does not clearly choose between them but rather lays out a policy scaffolding flexible enough for either to dominate depending on the outcome of future rulemaking and

stakeholder mobilization. The battle lines will not be purely technical but cultural: clinical conservatism versus digital agility, safety-by-design versus innovation-by-default, enterprise procurement versus consumer adoption.

In the coming years, CMS will face intense pressure to resolve these tensions. Every rule, guidance document, or procurement decision that flows from this RFI will become a proxy battlefield. Vendor lobbying will shape not only the regulatory treatment of digital health but its very ontology—whether it remains a supplementary character or becomes the new substrate of care delivery.

Next, I will finish the essay with the concluding analysis and synthesizing viewpoints.

The concluding analysis of this speculative essay brings us to the crossroads where health policy, technology infrastructure, and market ideology converge. The CMS Request for Information on the Health Technology Ecosystem is not merely a call for feedback; it is a provocation—an assertion that the state is no longer content to allow digital health to evolve organically within the confines of market inertia and siloed innovation. In the coming years, CMS and ONC appear poised to impose a coherent architecture, one rooted in interoperability mandates, identity verification systems, data liquidity norms, and patient-centered utility standards. This shift implies a philosophical repositioning of government from facilitator to orchestrator.

Incumbent vendors from across the health tech landscape will respond to this orchestration not with open rebellion, but with strategic adaptation and co-optation. They understand that regulation, when properly shaped, can become a competitive moat. Thus, their lobbying will not focus on resisting digital health modernization, but on scripting the terms of its implementation in ways that reinforce their incumbency. Whether through shaping the definition of “certified APIs,” steering TEFCA participation rules, controlling the rollout of digital identity infrastructure, or embedding proprietary data transformation services into otherwise open exchange models, these vendors will seek to dominate the policy stack just as they have dominated the technology stack.

In contrast, newer entrants and innovation-focused vendors will push for radical openness: unrestricted data flows, modular certification, lightweight regulatory expectations, and reimbursement systems that reward novel engagement rather than structural conformity. Their vision is expansive and consumer-centric, but also vulnerable to regulatory drag, fragmentation, and compliance fatigue. If CMS does not adopt agile policymaking paradigms that support these actors, the most creative innovations in digital therapeutics, patient engagement, and AI-enabled navigation may be stifled before they reach meaningful scale.

Payers, meanwhile, will continue their Janus-faced role—presenting themselves as patient advocates and quality champions to CMS, while simultaneously lobbying for data centralization, algorithmic opacity, and consent frameworks that privilege payer control over patient agency. Their ability to shape the conversation around quality metrics, prior authorization APIs, and real-time claims adjudication will profoundly influence whether digital health becomes a tool for empowering patients or simply a new layer of surveillance and behavioral conditioning.

Technology infrastructure providers—cloud platforms, middleware vendors, and normalization firms—will move in to capitalize on regulatory ambiguity. Their lobbying efforts will be less about ideology and more about position: ensuring that every new requirement CMS imposes creates a demand for services only they can fulfill. Whether this involves secure FHIR hosting, identity orchestration, or bulk data transformation, their goal will be to make themselves indispensable without being directly regulated.

The RFI's expansive reach into value-based care further complicates the equation. ACOs and other risk-bearing entities will seek to reframe digital health as an operational necessity, not a consumer product. Their lobbying will push CMS to view digital tools as levers for risk stratification, care coordination, and real-time quality reporting. This approach may drive broader adoption, but it risks embedding digital health inside the administrative logic of payment systems, stripping it of its potential to transform the lived experience of care.

In the final analysis, the digital health policy regime that emerges from this RFI not be decided solely by the merit of submitted comments or the vision of CMS technocrats. It will be the product of political contestation, stakeholder lobbying, the strategic maneuvering of incumbents determined to bend regulatory structure to their advantage. Whether this results in a vibrant, patient-empowered digital health ecosystem or a more interoperable but fundamentally conservative extension of today's infrastructure depends on how effectively CMS can balance inclusivity with rigor, innovation with safety, and competition with standardization.

If the agency succeeds in crafting a policy framework that is both technically robust and operationally flexible—one that welcomes new entrants without overburdening them, holds incumbents accountable without ossifying them, and enables patients to navigate their data landscape without being surveilled or manipulated—then this will mark the beginning of a new era in digital health. If not, it will simply codify the dominance of those best positioned to play the regulatory game.

Ultimately, CMS stands at a fork in the health technology road. The question is whether the digital health ecosystem will evolve, but who will write the code—technical, regulatory, and political—that determines what evolution means.



4 Likes • 2 Restacks

← Previous

Next

Discussion about this post

Comments

Restacks



Write a comment...