Public Comment on CMS–0042–NC: Health Technology Ecosystem RFI
Submitted by: Shannon Kennedy, Healthcare Chair, The Digital Economist
Professional Role: Chief Compliance Officer & Technology Strategist in Value-Based Care
Date: June 16, 2025
RIN: 0938–AV68

Executive Summary

As a leader in value-based care (VBC), compliance, and digital health innovation, I commend CMS and ASTP/ONC for advancing this critical dialogue on modernizing the health technology ecosystem. My comments reflect real-world experience working across full-risk Medicare/Medicaid models, integrating custom EHR systems, advancing interoperability, and supporting patient empowerment through digital health products world-wide. This response advocates for three transformative shifts: (1) empowering patients with complete self-custody of their medical records through blockchain-secured, QR code-accessible digital identity frameworks; (2) holding Certified EHR Technology (CEHRT) vendors and their clients accountable through verifiable compliance reporting rather than attestation; and (3) reframing risk stratification from a billing mechanism to a population health management tool that incentivizes real disease management and clinical outcomes.

I. PATIENT EMPOWERMENT THROUGH SELF-CUSTODY AND DIGITAL IDENTITY

The Vision: Complete Patient Ownership of Health Records

Responding to PC–2, PC–8, PC–10, and TD–13

Patients should have complete custodianship of their medical records—accessible, portable, and verifiable at the point of care. A QR code on a smartphone, printed card, or wearable should allow secure, consent-based access to complete health history without repeated clipboard exercises or fragmented portal access across multiple providers.

This vision must not remain aspirational—it must be imposed through federal mandate. CMS should establish a REAL ID–style framework for healthcare record portability. Just as TSA unified driver's license requirements, CMS can unify patient identity and data exchange standards across certified systems.

Policy Proposal: Blockchain-Based Patient Self-Custody

I recommend that CMS require every CEHRT-certified vendor to implement verifiable, QR code-based digital identity mechanisms that link to patient-controlled records. This framework should leverage blockchain or decentralized identifiers (DIDs) to allow patients to self-custody their records, determine access permissions, and log each access event immutably. Supporting research demonstrates the feasibility of this approach. The Estonia eHealth Foundation has successfully implemented blockchain-enabled health records at national scale, while projects like HIE of One and MedRec have proven the technical viability of patient-controlled health information exchange using blockchain architecture. TEFCA must evolve beyond provider-to-provider data exchange to incorporate self-custody nodes where patients hold an authoritative, verifiable copy of their longitudinal record and authorize temporary access via smart contracts or QR scans. This framework should include blockchain-based patient node options within

TEFCA governance, incentivize FHIR-enabled tools that allow read/write access from patient wallets, and include digital identity standards that allow biometric binding to digital health records.

II. CERTIFIED EHR ACCOUNTABILITY AND INTEROPERABILITY ENFORCEMENT

The Problem: Weaponized Trust Frameworks

Responding to TD–9, TD–10, PR–3, PR–6, and VB–13

Despite the intent of TEFCA and the 21st Century Cures Act, many CEHRT vendors are complicit in anti-competitive behavior that weaponizes the information blocking "privacy exception" and undermines interoperability under the guise of "trust frameworks." These practices deny legitimate care management access for population health organizations engaged in full-risk, value-based care, create administrative burdens by forcing providers to chase down faxes or engage in multiple logins for patient data already lawfully accessible under HIPAA's treatment/payment/operations provisions, and commercialize data exchange by requiring payers to purchase additional "payer platforms" to access patient data.

Policy Solution: From Attestation to Verification

Current provider attestation for interoperability creates a loophole—if providers attest "yes," they face no penalty, regardless of actual blocking behavior. CMS must replace attestation with a pass/fail certification test conducted by CEHRT vendors, measuring whether HIE endpoints are active, whether standards-based FHIR APIs are open and responding to external queries, whether TEFCA participation is implemented correctly, and whether use-based permissions for treatment, payment and operations are functioning – not just treatment. Federalism has the state-imposed HIE opt-in or opt-out managed for the patients; therefore, any outcry by actors to protect patient privacy in the name of “trust” and over impose unnecessary authorizations, which only cost taxpayers more money, must be eliminated.nCertified EHRs must become whistleblowers by design, required to report to CMS which of their clients have turned off interoperability functionality, when access is restricted via private "trust" frameworks that deviate from TEFCA, and when clients are deliberately suppressing data exchange under false privacy pretenses. This naturally disincentivized Certified EHRs from forming their own “rules of the road” with their constituents that likewise arbitrage information blocking prohibitions in the name of misguided privacy exceptions. It is not uncommon for large healthcare systems to deliberately block electronic access to health records for payment and operations as a punishment in payer contract negotiations. This practice must be stopped. Additionally, payers should also be interoperable actors and CMS should continue with momentum on pursuing bad-acting with denied claims and egregious prior-authorization practices in those relevant payer rules.

Payer Accountability Under the Cures Act

Responding to PA–1 through PA–5

CMS should explicitly designate payers as "actors" under the 21st Century Cures Act's Information Blocking provisions and subject them to both technical and compliance obligations. This includes mandating adoption of all CAQH CORE Phase IV, V, and VI operating rules,

requiring that all standard electronic transactions be exposed via public, standards-based APIs rather than proprietary payer portals, and enforcing API uptime, response time, and error transparency rules comparable to banking standards.

III. TRANSFORMING RISK STRATIFICATION TO POPULATION HEALTH MANAGEMENT

Beyond RAF Score Inflation

Responding to VB–1 through VB–4

Traditional risk stratification models in Medicare Advantage, ACOs, and other Alternative Payment Models are overly dependent on claims-derived predictive analytics that fail to translate into effective care. These models serve as a proxy for RAF score inflation rather than clinical decision-making, resource prioritization, or patient engagement. Despite billions invested across the system, the causal relationship between stratification and population health improvement remains largely unproven.

A New Framework: Population Health Management Impact

CMS should replace the narrow RAF-focused stratification paradigm with a Population Health Management Impact Framework (PHM-IF) that shifts focus from predicted cost to intervention impactability, incentivizes models that demonstrate real clinical improvement such as medication adherence and blood pressure control, and incorporates impactibility modeling that targets patients most likely to benefit from outreach. This framework should tie risk adjustment revenue to documented case management activities, require vendors and providers to log interventions at the patient level, and introduce a case management multiplier where risk score payment is scaled based on case management evidence submitted.

IV. DIGITAL HEALTH LITERACY AND ACCESSIBILITY

Mandating Health Literacy Support Tools

Responding to PC–1, PC–4, PC–5, PC–6

Digital tools that support health literacy should be mandated components of all CMS-certified portal experiences for both members and patients. These tools are critical for ensuring meaningful access to benefits, navigating complex medical documentation, and increasing health equity in populations most likely to face barriers due to literacy, language, disability, or digital exclusion. AskMia.com exemplifies technology done right in this space. This AI-powered literacy assistant reads insurance documents aloud, translates content, and explains benefits in plain language. Currently used by forward-thinking Medicare Advantage and Medicaid MCOs, AskMia features a "smart highlighter" to show definitions and next steps, voice support, and an embeddable widget for payer and provider portals. The platform is HIPAA compliant and tailored specifically to health plan documents, making it more robust than generic AI assistants for healthcare applications. Over 88% of U.S. adults are not proficient in health literacy, and low health literacy is linked to poorer health outcomes, higher costs, and more avoidable hospitalizations. A 2022 analysis found that 94% of Summary of Benefits and Coverage documents exceeded the recommended 8th-grade readability level, making true comprehension impossible without active navigation support. CMS should require all certified

portals to include embedded health literacy assistants, real-time translation and read-aloud tools, and literacy-adjusted navigators for benefit explanations. This requirement should be tied to CMS certification for patient-facing technology, MA plan compliance with member materials standards, and provider portal incentives under CEHRT certification.

V. ARTIFICIAL INTELLIGENCE GOVERNANCE AND MEDICAL AI

Domain-Specific Medical AI Priority
Responding to TD–8, TD–9, VB–2

Not all AI is created equal. While general-purpose large language models like GPT-4 have wide applicability, they are not trained to safely operate in clinical environments. Medical decision-making requires understanding of clinical ontologies, sensitivity to risk/benefit tradeoffs, and adherence to clinical guidelines. CMS and ONC should develop a differentiated AI certification pathway for models that are purpose-built and pretrained on de-identified clinical corpora, designed for clinical utility and patient navigation, and built in alignment with HIPAA and 21st Century Cures Act requirements. GeneHealth.ai represents an exemplary model of this approach—a large medical model (LMM) built specifically for the health sector. Unlike general-purpose AI, GeneHealth.ai is pretrained on billions of tokens of medical text including de-identified EHRs, biomedical research, and clinical notes. The platform is architected with native support for clinical reasoning tasks including summarization, coding, prior authorization explanation, clinical documentation, and care gap detection. Critically, it integrates clinical guardrails, audit logs, and prompt security layers specifically designed for regulatory compliance and traceability in healthcare environments. Such domain-specific models should be eligible for fast-track ONC certification and included in CMS demonstrations for AI governance, representing the gold standard for responsible AI implementation in healthcare. CMS should establish an AI Model Registry under ONC requiring registration of any model used in CEHRT-certified tools, create certification tracks for Large Medical Models demonstrating accuracy on clinical vignettes, and prioritize investment in domain-specific AI through the CMS Innovation Center.

Productive Edge exemplifies the type of responsible AI governance framework that should be mandated industry-wide. Their Responsible AI for Healthcare Strategy provides frameworks for scoring AI tools for fairness and safety, serving as "sentinel layers" to detect and prevent algorithmic manipulation or discrimination, and supporting organizations in implementing ethical AI practices. CMS should fund RFPs for AI Governance Technology to create “certified vendors” that can provide accountability infrastructure for the responsible deployment of AI in healthcare and become the next best-practice governance tool that ensures AI performance observation is occurring.

VI. VALUE-BASED CARE TECHNOLOGY REQUIREMENTS

Essential Capabilities for VBC Success
Responding to VB–3, VB–4, VB–11

Essential health IT capabilities for value-based care include real-time patient matching across CMS and provider systems, longitudinal care plan updating across episodes, remote biometric device support, predictive analytics for HCC gap closure, and blockchain-integrated personal health records with smart contracts for record access. Current certification criteria should be enhanced to require stratified tech requirements for rural versus urban APMs, use of open-source CEHRT alternatives, and allowing high-functioning HIEs as intermediaries in meeting FHIR endpoint access goals.

VII. SPECIFIC POLICY RECOMMENDATIONS

Immediate Actions for CMS

1. Mandate Patient Self-Custody Infrastructure: Require CEHRT vendors to implement QR code-based, blockchain-secured patient record access within 24 months.

2. Implement Verified Compliance Reporting: Replace provider attestation with vendor-conducted certification tests measuring actual interoperability functionality.

3. Designate Payers as Cures Act Actors: Subject payers to Information Blocking enforcement and mandate CAQH CORE operating rules adoption.

4. Establish Medical AI Certification Track: Create differentiated pathways for domain-specific healthcare AI models with clinical guardrails.

5. Launch Population Health Impact Framework: Pilot PHM-IF in Medicare Advantage and ACO programs, tying payment to documented case management outcomes.

6. Mandate Health Literacy Support: Require embedded literacy assistants in all certified patient-facing portals.

Long-term Vision

CMS is positioned to create a patient-first, technology-enabled health infrastructure by incentivizing FHIR-compatible tools linked to value-based care models, expanding the Blue Button API to support richer use cases, lowering barriers for digital engagement, and enforcing anti-information-blocking policies with accountability.

Conclusion

The federal government has invested billions in CEHRT adoption and health IT infrastructure. It is time to shift from "trust us" to "prove it" accountability, empower patients with true ownership of their health data, and align technology requirements with actual health outcomes rather than administrative convenience. I appreciate the opportunity to respond and welcome the opportunity to further support this transformative work through continued engagement with CMS and ASTP/ONC leadership.

Bibliography

1. Ekblaw, A., Azaria, A., Halamka, J.D., & Lippman, A. (2016). A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. MIT Media Lab.
2. Estonia eHealth Foundation. Blockchain-enabled eHealth System. Available at: https://e-estonia.com/solutions/healthcare/e-health-record/
3. HIE of One Project. Patient-directed HIE using OAuth and Blockchain. Available at: https://hieofone.org
4. Berkman ND, Sheridan SL, Donahue KE, et al. (2011). Health Literacy Interventions and Outcomes: An Updated Systematic Review. Evidence Report/Technology Assessment No. 199. AHRQ Publication No. 11-E006.
5. Kutner M, Greenberg E, Jin Y, Paulsen C. (2006). The Health Literacy of America's Adults: Results from the 2003 National Assessment of Adult Literacy (NAAL). NCES.
6. PlainLanguage.gov. (2022). Toolkit for Making Written Material Clear and Effective: Readability Analysis of Insurance Materials.
7. Adler-Milstein, J., & Pfeifer, E. (2017). Information Blocking: Is it occurring and what policy strategies can address it? Milbank Quarterly, 95(1), 117–135.
8. 21st Century Cures Act, §4004 – "Interoperability and Information Blocking." Available at: https://www.congress.gov/bill/114th-congress/house-bill/34
9. CAQH CORE Operating Rules Summary. Available at: https://www.caqh.org/core
10. HL7 Da Vinci Project. Available at: https://www.hl7.org/about/davinci/
11. GeneHealth.ai (2024). Building a Medical Foundation Model for Clinical Utility. Available at: https://www.genehealth.ai
12. Obermeyer, Z. et al. (2019). "Dissecting racial bias in an algorithm used to manage the health of populations." Science.
13. W3C. (2022). Decentralized Identifiers (DIDs) v1.0. Available at: https://www.w3.org/TR/did-core/
14. Sovrin Foundation. (2021). Self-Sovereign Identity (SSI) and Healthcare Use Cases. Available at: https://sovrin.org
15. Productive Edge. (2023). Responsible AI for Healthcare Strategy. Available at: https://productiveedge.com
16. AskMia.com – AI-powered health literacy assistant. Available at: https://askmia.com