CDC Data Intermediaries RFI Comment — Data Quality Certification as Universal Intermediary Baseline

Public Comment on Request for Information: Data Intermediaries and Approaches to Strengthen Public Health Data Exchange

Re: CDC-2026-1519, 91 FR 59777 (September 21, 2026)

Submitted by: Box Commons 30 N Gould St Ste N Sheridan, WY 82801 Contact: Brice Love, Founding Catalyst Email: info@boxcommons.org Web: boxcommons.org

Date: September 30, 2026

Submitted via: regulations.gov (PDF attachment)

Docket: Data Intermediaries and Approaches to Strengthen Public Health Data Exchange, CDC-2026-1519, 91 FR 59777 (September 21, 2026). Statutory authority: 42 U.S.C. § 241, § 247d-4.

I. Executive Summary

Box Commons respectfully submits this comment on the Centers for Disease Control and Prevention's Request for Information regarding data intermediaries and approaches to strengthen public health data exchange.

Box Commons is a 501(c)(6) standards body developing technology-agnostic certification standards for data used in AI systems, governed by a three-chamber structure (Industry, Civil Society, Academic/Research) with equal voting weight to prevent capture by any single interest group. Full organizational details appear in Section IX below.

Our central observation: The health data exchange ecosystem has achieved a robust, independently certified infrastructure for *cybersecurity* — most notably through the HITRUST certification required by TEFCA Common Agreement Section 12.1.2 for all Qualified Health Information Networks (QHINs). No analogous certification exists for *data quality, accuracy, or provenance*. HITRUST certifies the pipe. Nobody certifies the water. As data intermediaries increasingly feed AI training pipelines for clinical decision support, prior authorization, and public health surveillance, this asymmetry exposes the entire ecosystem to compounding risks: clinically incoherent training data, legally indefensible consent chains, algorithmically amplified bias, and an insurance market that is systematically withdrawing coverage for AI-related liability.

Our central recommendation: The CDC should incorporate independent, third-party data quality and provenance certification as a core component of the proposed Universal Intermediary

Baseline. Specifically, we recommend that the CDC:

1. Recognize data quality certification — analogous to HITRUST for cybersecurity — as a baseline capability for public health intermediaries, extending beyond format standardization (USCDI) to encompass accuracy, completeness, consent provenance, and AI-readiness;
2. Adopt the NCQA Data Aggregator Validation (DAV) program as a foundation for intermediary assessment, extended with provenance and AI-readiness criteria that DAV does not currently address;
3. Establish tiered certification maturity levels that provide intermediaries a structured pathway from basic USCDI compliance to full AI-readiness certification;
4. Condition any certification framework on multi-stakeholder governance with structural safeguards against vendor capture, including balanced voting weight, royalty-free intellectual property defaults, and funded adversarial participation; and
5. Recognize that independent certification resolves the information asymmetry that self-attestation cannot address — a position we have articulated across 22 public comments to 14 federal, state, and international agencies, most recently to the Colorado Attorney General regarding the Automated Decision-Making Technology Act (4 CCR 904-6, September 23, 2026) and to the FCC regarding the Robocall Mitigation Database (FCC 26-49, WC Docket Nos. 24-213 and 17-97, September 23, 2026).

II. The Industry Need: Why Data Quality Certification Cannot Wait

Before addressing the RFI's specific questions, we present the convergent pressures that make data quality certification an urgent infrastructure requirement — not for any single organization, but for the healthcare industry as a whole.

Providers cannot comply with HTI-1 without certified intermediary data. ONC's Health Data, Technology, and Interoperability rule (HTI-1) requires EHR developers to expose 31 source attributes about their predictive AI, including demographic representativeness and fairness metrics. If intermediaries strip that metadata during aggregation and de-identification, developers cannot populate those required fields. Data quality certification for intermediaries resolves a compliance problem that providers and developers already face.

Insurers cannot defend their AI determinations in court without it. In *Estate of Lokken v. UnitedHealth Group* (Case No. 0:23-cv-03514, D. Minn. 2026), the court permitted discovery into the training data quality and accuracy rates of UnitedHealth's nH Predict algorithm, which plaintiffs alleged systematically denied post-acute care coverage. The court did not evaluate the algorithm's sophistication — it asked whether the *data* was accurate and individualized. Every major insurer using AI for prior authorization now faces the same evidentiary demand. Certified data provenance from intermediaries provides a defensible answer.

State algorithmic governance frameworks require it. Colorado Regulation 10-1-1 mandates bias testing on AI used in insurance benefit determinations. Bias testing requires demographic metadata. If Safe Harbor de-identification stripped that metadata upstream, bias testing is mathematically impossible. Provenance certification does not re-inject demographics into patient records — it documents the *composition profile* of the dataset so that bias auditing can proceed. Colorado is the first; it will not be the last.

CDC's own AI strategy depends on it. The CDC's 2026 Public Health Data Strategy envisions

predictive surveillance capabilities — disease detection, outbreak modeling, resource allocation — built on intermediary-sourced data. Data quality failures in those pipelines produce flawed predictions. During an active outbreak, that is not an abstract quality concern. The Universal Intermediary Baseline proposed in this RFI is the right vehicle to build data quality certification before AI pipelines are fully operational, not after a failure forces it.

Intermediaries themselves need the insurance pathway. ISO/Verisk exclusionary endorsements CG 40 47 and CG 40 48, adopted by an estimated 95 percent of carriers since January 2026, strip AI-related liability from standard commercial general liability coverage. Intermediaries deploying machine learning for record matching, entity resolution, and deduplication — core operational functions — are likely operating without CGL coverage for those activities. Certification against published standards establishes the documented standard of care that specialty AI insurers require before writing a policy.

On the cost objection. NCQA DAV already operates at known cost — a 12-to-18-week validation cycle, not an exotic process. The tiered model we propose below begins at Tier 1 (USCDI compliance most intermediaries already achieve), so incremental cost of entry is low. The cost of *not* certifying is demonstrably higher: litigation discovery costs (as *Lokken* illustrates), regulatory non-compliance penalties (HTI-1, Colorado), and uninsurable operations. The relevant comparison is not certification cost versus zero — it is certification cost versus the cost of the status quo.

III. The Data Quality Certification Gap

A. TEFCA's Asymmetric Mandate

The Trusted Exchange Framework and Common Agreement (TEFCA), operationalized under the 21st Century Cures Act and governed by The Sequoia Project as the Recognized Coordinating Entity, represents the federal government's most ambitious effort to create a single on-ramp for nationwide health information interoperability. TEFCA excels in establishing a highly secure transport layer.

Section 12.1.2 of the Common Agreement requires independent third-party security certification for all QHINs. In practice, HITRUST has emerged as the designated cybersecurity certifier, auditing compliance against NIST SP 800-53 and HIPAA security rules. DirectTrust administers the Accredited Trust Anchor Bundle (ATAB) and provides Registration Authority credentialing at IAL2/AAL2 assurance levels.

However, TEFCA enforces no analogous third-party certification for the quality, accuracy, or provenance of the clinical data flowing through these secure channels. The TEFCA Standard Operating Procedures dictate formatting and permitted uses of data — Treatment, Payment, Health Care Operations, Public Health — but do not mandate that the data payload itself be clinically coherent, deduplicated, or semantically normalized.

The United States Core Data for Interoperability (USCDI) v3 standardizes the *format* of exchanged data elements. It does not certify the *accuracy* of their content. A USCDI-compliant data exchange can transmit perfectly formatted records that are clinically inaccurate, duplicated, or stripped of the provenance metadata necessary for downstream AI use.

B. The NCQA DAV Precedent — And Its Limits

The National Committee for Quality Assurance (NCQA) established the Data Aggregator Validation (DAV) program to evaluate the ingestion, transformation, and output of aggregated clinical data by HIEs, HDUs, and other intermediaries. DAV is the closest existing analogue to "HITRUST for data quality."

The DAV validation cycle is a rigorous 12-to-18-week process comprising three core components:

1. **Process Standards Review:** Assessment of the intermediary's data management governance, coding integrity, quality assurance, and change management from the point of ingestion.
2. **System Conformance:** Testing outbound data streams against NCQA HL7 C-CDA or FHIR Implementation Guides for strict technical alignment.
3. **Primary Source Verification (PSV):** Intensive audit comparing sample cases directly against the legal medical record in the originating clinical source.

DAV-certified intermediaries — such as HealthShare Exchange in Pennsylvania and HealtHIE Nevada — produce data streams that health plans can utilize as "standard supplemental data" for HEDIS reporting, eliminating the need for manual chart chases and downstream PSV audits by payers. DAV demonstrates that rigorous, third-party certification of clinical data quality is technically feasible for intermediaries.

However, DAV certifies *fidelity to the source record*. It does not certify *suitability for AI training*. DAV confirms that the intermediary faithfully reproduced what the EHR contained. It does not assess whether the underlying data is demographically representative, whether consent chains are intact for secondary AI use, whether de-identification has stripped the provenance metadata necessary for fairness testing, or whether the data carries the temporal and geographic granularity required for bias auditing.

C. The Sequoia DUWG — Voluntary, Not Mandatory

The Sequoia Project's Data Usability Workgroup (DUWG) Implementation Guide V2.0, finalized in late 2024, addresses critical data quality challenges including provenance traceability ("Who, What, When, Where, How, Why"), duplicate reduction, and reconciliation of narrative versus discrete clinical data. The Guide represents thoughtful, technically rigorous work.

However, the DUWG Guide operates as a voluntary "Taking Root" movement, not a certification prerequisite for TEFCA participation. Its adoption is uneven and unaudited. The result: TEFCA currently guarantees that data is transmitted securely by authenticated actors, but offers no institutional guarantee that the data is accurate, complete, or suitable for secondary use.

Feature	TEFCA/HITRUST (Current)	Data Quality Certification (The Gap)
Certifying entities	HITRUST, DirectTrust	NCQA (DAV), specialized auditors
Regulatory enforcement	Mandated (Common Agreement §12.1.2)	Voluntary (Sequoia DUWG)
Verification focus	Encryption, identity proofing, access controls	Semantic accuracy, deduplication, provenance

AI impact	Prevents interception and unauthorized access	Ensures training data is clinically accurate and unbiased

---

IV. Responses to Specific RFI Questions

A. Section II.B, Question 2 — Universal Intermediary Baseline Capabilities

The RFI asks which core capabilities should constitute the Universal Intermediary Baseline. We recommend that **independent data quality and provenance certification** be included as a baseline capability alongside cybersecurity, identity proofing, and transport-layer interoperability.

Data quality certification should encompass four elements:

1. **Semantic accuracy** — clinical data elements faithfully represent the source encounter, validated through PSV methodologies analogous to NCQA DAV;
2. **Provenance integrity** — the chain of custody from originating clinical source through each intermediary transformation is documented and verifiable, consistent with AMIA's recommendation that ONC make "provenance" a functional requirement comprising both "path" (how data traveled from originator) and "validity" (hash/checksum verification);
3. **Consent documentation** — for data entering secondary use pathways including AI training, verifiable records that appropriate authorization exists under HIPAA or applicable state law; and
4. **Demographic representativeness metadata** — sufficient granularity to support the fairness and bias testing required by ONC HTI-1 FAVES and state algorithmic governance frameworks such as Colorado Regulation 10-1-1.

The FHIR R4 Provenance Resource provides the technical substrate for implementing these capabilities but is not currently mandated. We recommend the CDC require intermediaries to support the FHIR Provenance Resource as a condition of the Universal Baseline.

B. Section II.B, Question 3 — Assessment and Certification Mechanisms

The RFI asks how intermediary capabilities should be assessed and certified. We propose a **four-element conformance pattern** that we have recommended across multiple federal dockets:

1. **Published technical criteria** — version-controlled standards against which intermediaries can be assessed, building on NCQA DAV methodology and the Sequoia DUWG Implementation Guide;
2. **Independent conformance assessment** by accredited bodies operating under ISO/IEC 17065 (conformity assessment) and ISO/IEC 17011 (accreditation body requirements);
3. **Machine-readable, cryptographically verifiable credentials** — structured records that a specified intermediary, as of a specified date, meets specified criteria as confirmed by a specified assessor; and
4. **Continuous conformance** through periodic reassessment or continuous reporting, ensuring credentials reflect current system configurations rather than a point-in-time snapshot.

This pattern is proven in adjacent federal contexts: FedRAMP for cloud security, FIPS 140-3 for cryptographic module validation, Common Criteria for product certification, and HITRUST itself for healthcare cybersecurity. Extending it to data quality is architecturally straightforward because the

compliance infrastructure — accreditation bodies, assessment methodologies, credential registries — already exists.

The NCQA DAV program provides a strong methodological foundation. We recommend extending DAV with three additional assessment domains that it does not currently address:

Assessment Domain	NCQA DAV (Current)	Proposed Extension
Source fidelity	PSV audits against originating EHR	Retain — core methodology
AI-readiness	Not assessed	Consent chain verification for secondary AI use
Provenance survivability	Not assessed	Metadata retention through de-identification
Demographic adequacy	Not assessed	Representativeness profiling for bias testing

C. Section II.B, Question 4 — Maturity Model

The RFI asks about maturity models for intermediary development. We recommend a **three-tier certification model** that provides intermediaries a structured pathway:

Tier 1 — Baseline Compliance. USCDI conformance, HITRUST cybersecurity certification, and FHIR Provenance Resource support. This tier reflects current TEFCA requirements extended with mandatory provenance metadata.

Tier 2 — Data Quality Certification. NCQA DAV-equivalent validation including PSV audits, semantic accuracy verification, and duplicate reconciliation. This tier certifies that intermediary output faithfully represents source clinical data.

Tier 3 — AI-Readiness Certification. Full provenance chain documentation, consent verification for secondary AI use, demographic representativeness profiling, and metadata survivability assessment through de-identification. This tier certifies that intermediary data is suitable for downstream AI training and meets the source attribute requirements of ONC HTI-1 FAVES.

This tiered approach allows intermediaries to progress incrementally while creating a visible, measurable pathway toward the data quality infrastructure that the healthcare AI ecosystem requires.

D. Section II.B, Question 5 — Impact of AI on Intermediary Requirements

The emergence of AI in healthcare — for clinical decision support, prior authorization, claims processing, and public health surveillance — fundamentally changes what intermediaries must certify about their data.

De-identification destroys provenance. HIPAA Safe Harbor (§164.514(b)) requires removal of 18 categories of identifiers including geographic subdivisions, date elements, and biometric identifiers. While essential for privacy, Safe Harbor strips the temporal and demographic metadata that AI developers need to comply with ONC HTI-1 FAVES requirements for training data representativeness and fairness testing. The Expert Determination method (§164.514(a)) preserves more clinical utility but provides no standardized mechanism for downstream recipients to verify *what* was retained and

how re-identification risk was assessed. The result: data intermediaries deliver AI-ready data in a format that makes AI compliance technically impossible.

The consent crisis. In *Washington v. Sutter Health* (Case No. 4:26-cv-03012, N.D. Cal. 2026), plaintiffs alleged that health systems using Abridge AI's ambient documentation platform recorded patient-physician conversations and transmitted audio files to external servers without obtaining explicit all-party consent. The court held that a HIPAA Business Associate Agreement does not immunize a health system or its AI intermediary from state wiretapping and consumer privacy laws, which carry statutory damages of $5,000 per violation under the California Invasion of Privacy Act. For public health intermediaries, this precedent means that clinical notes generated by ambient AI scribes — a rapidly growing category of data entering intermediary pipelines — carry unverifiable consent chains that expose the entire downstream ecosystem to legal liability.

Algorithmic claims denial litigation. In *Estate of Lokken v. UnitedHealth Group* (Case No. 0:23-cv-03514, D. Minn. 2026), the court denied dismissal and permitted discovery into the technical architecture, training data, and accuracy rates of UnitedHealth's nH Predict algorithm, which plaintiffs alleged systematically denied post-acute care coverage. Post-acute denial rates doubled after the algorithm's deployment. The *Lokken* precedent establishes that courts will require insurers to demonstrate that their AI determinations are based on accurate, individualized, and high-quality clinical data — creating direct demand for certified data quality from intermediaries.

These developments establish that data intermediaries feeding AI pipelines cannot be evaluated solely on transport security and format compliance. The Universal Intermediary Baseline must account for the downstream consequences of data quality failures in AI applications.

E. Section II.C, Question 4 — Open Standards and Vendor Lock-In

The RFI asks about mechanisms to ensure open standards and prevent vendor lock-in. We recommend three structural safeguards:

Royalty-free intellectual property defaults. Any certification framework for public health intermediaries should require that participating standards be available on royalty-free terms. Standards that create preferences for patented technologies introduce vendor dependency by design. Box Commons has pledged its entire AI credentialing patent portfolio — 12 patents across four omnibus filings — on royalty-free terms, establishing that this model is commercially viable for standards-body operations.

Technology-agnostic, outcome-based criteria. Certification standards should specify *what* intermediaries must achieve (data accuracy thresholds, provenance completeness, consent chain verification), not *how* they must achieve it. Prescriptive technology mandates create lock-in; outcome-based criteria allow innovation while maintaining accountability.

Interoperability by design. Certification credentials issued to intermediaries should be machine-readable, standards-based (e.g., W3C Verifiable Credentials, FHIR-native), and queryable through open registries. Proprietary credential formats create a second-order lock-in that is more durable and more difficult to escape than the first.

F. Section II.D, Question 1 — Governance Structures

The RFI asks about governance structures for intermediary oversight. We recommend that any body developing data quality certification standards for public health intermediaries operate under

multi-stakeholder governance with structural anti-capture mechanisms.

The challenge is specific: data intermediaries are simultaneously the entities being certified and, in many standards processes, the entities writing the certification criteria. Single-stakeholder governance — where industry participants control the standards process — creates a structural conflict of interest that erodes certification credibility.

Box Commons addresses this through a three-chamber governance model:

- **Industry Chamber** — technology vendors, data intermediaries, health systems, and insurers;
- **Civil Society Chamber** — patient advocates, community organizations, and public health practitioners; and
- **Academic/Research Chamber** — clinical researchers, informaticists, and independent technical experts.

Each chamber holds equal voting weight. No single chamber — and no single entity within any chamber — can unilaterally determine standards outcomes. This structure, modeled on the Forest Stewardship Council, ensures that the entities being certified do not control the certification criteria.

G. Section II.D, Question 2 — Safeguards Against Conflicts of Interest

The RFI asks about safeguards against conflicts of interest and vendor lock-in. We recommend four structural mechanisms:

1. **Funding cap:** No single entity may provide more than 25 percent of the certifying body's annual revenue, preventing financial dependency on any participant.
2. **Cooling-off periods:** Individuals transitioning from regulated entities to governance roles in the certifying body must observe a defined separation period.
3. **Funded adversarial participation:** The certifying body should allocate resources to fund participation by consumer advocates and independent researchers who would otherwise lack the resources to engage in standards processes — ensuring that the governance structure is not nominally multi-stakeholder but effectively industry-dominated.
4. **Annual independence audit:** A public assessment of governance composition, funding sources, and voting patterns, demonstrating that the certifying body's independence is maintained in practice, not merely in bylaws.

V. The Insurance Forcing Function

Independent of any regulatory mandate, the insurance market is creating economic pressure for data quality certification that public health intermediaries cannot ignore.

A. The AI Liability Exclusion Wave

As we documented in our September 2026 comments to the Colorado Attorney General (4 CCR 904-6) and the FCC (FCC 26-49), Verisk/ISO released exclusionary endorsements CG 40 47 and CG 40 48 in January 2026, broadly excluding AI-related liability from standard commercial general liability coverage. CG 40 47 categorically strips Coverage A (bodily injury and property damage) and Coverage B (personal and advertising injury) for any claim "arising out of" generative AI. Industry estimates indicate 95 percent carrier adoption.

These exclusions apply directly to health data intermediaries deploying AI-based data quality, deduplication, or transformation tools — which is to say, they apply to the modern intermediary's core operational stack. An intermediary that uses machine learning for record matching, entity resolution, or semantic normalization operates AI systems that its CGL carrier has likely excluded from coverage.

B. Specialty Coverage Requires Certified Provenance

Specialty AI insurers — including Armilla (Lloyd's-backed, up to $25 million), Munich Re's HSB (up to $10 million E&O), and Testudo (Lloyd's Lab, mid-market) — require auditable governance and data provenance verification as conditions of coverage. An intermediary that certifies its data quality practices against published standards establishes a defensible standard of care and provides the documentation necessary for insurance brokers to negotiate affirmative coverage or secure standalone AI liability policies.

For public health intermediaries, the insurance forcing function reinforces the regulatory case: certified data quality is not merely a quality improvement initiative. It is a commercial necessity for intermediaries seeking to maintain insurable operations as AI becomes embedded in their workflows.

VI. Cross-Domain Evidence: Data Certification in Operation

Box Commons operates a live data certification pipeline — the BC-Certified Audio Data Standard — across a 22-station broadcast radio network.

A. What BC-Certified Demonstrates

The pipeline captures live broadcast streams, parses playout metadata, performs audio fingerprinting for copyrighted content identification, reconciles scheduled-versus-actual content, and generates tamper-evident audit trails with SHA-256 hashing at ingestion. Consent documentation follows a structured schema covering rights holder identity, content scope, permitted uses, and revocation terms. These tools are open-source and inspectable.

B. Why Broadcast Radio Validates Health Data Intermediaries

Broadcast radio presents a more technically demanding certification environment than health data exchange:

Dimension	Broadcast Radio	Health Data Exchange
Volume	22 stations, continuous 24/7 streams	Batch and event-driven message exchange
Latency	Real-time stream capture and processing	Asynchronous processing windows
Content diversity	Music, speech, ads, station IDs, weather	Structured clinical documents (C-CDA, FHIR)
Format variability	Multiple streaming codecs, bitrate variation	Standardized (HL7, FHIR, C-CDA)

Health data exchange benefits from standardized formats (HL7, FHIR, C-CDA) and structured content that broadcast radio lacks. If data quality certification works for the higher-volume, higher-complexity, less-standardized broadcast radio environment, the certification infrastructure generalizes to health data intermediaries with substantially less technical overhead.

VII. Recommendations

We respectfully recommend that the CDC:

1. **Include data quality certification in the Universal Intermediary Baseline.** The proposed Framework should recognize data quality and provenance certification — analogous to HITRUST for cybersecurity — as a core intermediary capability. Format compliance (USCDI) and transport security (HITRUST) are necessary but insufficient; the baseline should also encompass semantic accuracy, provenance integrity, and consent chain verification.

2. **Adopt and extend the NCQA DAV methodology.** The DAV program provides a proven, operational model for intermediary data quality certification. The CDC should work with NCQA and other stakeholders to extend DAV with AI-readiness criteria including consent chain verification, demographic representativeness profiling, and provenance metadata survivability through de-identification.

3. **Establish tiered certification maturity levels.** A three-tier model — from baseline USCDI compliance through DAV-equivalent data fidelity to full AI-readiness certification — provides intermediaries a structured pathway and allows the CDC to set progressively higher expectations as the intermediary ecosystem matures.

4. **Require FHIR Provenance Resource support.** The FHIR R4 Provenance Resource provides the technical substrate for data quality certification but is not currently mandated. Requiring intermediaries to support it as a baseline capability creates the infrastructure on which certification programs can operate.

5. **Condition certification frameworks on multi-stakeholder governance.** Any body developing data quality certification standards should meet defined governance criteria: multi-stakeholder participation with balanced voting weight, intellectual property policies defaulting to royalty-free terms, separation of standards development from certification assessment, and publicly accessible certification registries.

6. **Address AI-specific risks in intermediary assessment.** The Universal Intermediary Baseline should explicitly account for the downstream consequences of data quality failures in AI applications — including the de-identification provenance paradox, the consent crisis exposed by ambient AI scribe litigation, and the data quality demands created by ONC HTI-1 FAVES and state algorithmic governance frameworks.

VIII. Standing Offer

Box Commons offers to participate, at no cost, in any technical advisory process, pilot program, or working group the CDC convenes to develop data quality certification standards for public health intermediaries. We can demonstrate our data certification pipeline against live broadcast audio

streams, share our open-source tooling, and provide technical input on how data quality certification architectures proven in one domain can be adapted to health data exchange.

IX. About Box Commons

Box Commons is a 501(c)(6) standards body headquartered in Wyoming. We develop technology-agnostic, outcome-based certification standards for data used in AI systems — certifying observable data quality, consent documentation, and audit trail integrity, not mandating specific technologies or architectures.

Governance: Three-chamber system (Industry, Civil Society, Academic/Research) with equal voting weight, modeled on the Forest Stewardship Council. No single entity controls the standards process.

IP Policy: Royalty-free default. All AI credentialing patents from the founding portfolio are pledged RF. Standards never create preferences for any patented technology.

Standards alignment: ISO/IEC 5259-2 and 5259-4 (data quality for ML), C2PA (content provenance), EBUCore (broadcast metadata), IPTC Digital Source Type, IAB Podcast Measurement Guidelines, NIST AI RMF.

Prior CDC/HHS engagement: This is Box Commons' first comment to the CDC. We have previously engaged HHS through the NIST AI agent security RFI (CAISI, March 2026 — acknowledged by Drew Keller), the NIST NCCoE Identity and Authorization concept paper (March 2026), and the NIST AI 800-2 proceeding (March 2026).

Broader regulatory engagement: 22 public comments filed across 14 federal, state, and international agencies, including NIST, NHTSA, NAIC, FCC, SEC, GSA, Colorado AG, and Singapore IMDA. Acknowledged by NIST CAISI team (March 2026).

Respectfully submitted,

Brice Love
Founding Catalyst
Box Commons
info@boxcommons.org
boxcommons.org

AI Disclosure: This comment was prepared with AI assistance. Methodology: analysis of CDC RFI CDC-2026-1519 (91 FR 59777); review of TEFCA Common Agreement and QHIN Technical Framework; assessment of NCQA Data Aggregator Validation program; analysis of ONC HTI-1 FAVES transparency requirements; review of Sequoia Project DUWG Implementation Guide V2.0 and AMIA provenance recommendations; examination of FHIR R4 Provenance Resource specifications; synthesis of case law including Estate of Lokken v. UnitedHealth Group (0:23-cv-03514, D. Minn. 2026) and Washington v. Sutter Health (4:26-cv-03012, N.D. Cal. 2026); insurance market analysis of ISO/Verisk exclusionary endorsements (CG 40 47/48); review of NAIC Model Bulletin, Colorado SB 21-169, and CMS-0057-F Prior Authorization Rule; drafted by Claude (Anthropic) under human

direction and review. All factual claims were independently verified before inclusion. The analytical framework, strategic positioning, and policy recommendations reflect the judgment of the human author.