Submitted Electronically

November 20, 2026

The Honorable Erica Schwartz, MD, MPH, JD (RADM, USPHS, RET)
Centers for Disease Control and Prevention
U.S. Department of Health and Human Services
1600 Clifton Road NE
Atlanta, GA 30329

RE: RFI—Data Intermediaries and Approaches to Strengthen Public Health Data Exchange

Dear Dr. Schwartz:

The American Medical Informatics Association (AMIA) appreciates the opportunity to comment on the Centers for Disease Control and Prevention's (CDC) request for information (RFI) regarding data intermediaries and approaches to strengthen public health data exchange. AMIA is the professional home for more than 8,000 informatics professionals who apply the science of informatics to advance health, healthcare, research, and public health. Our members work across clinical and public health informatics, information standards, research, system implementation, governance, and evaluation.

AMIA supports CDC's exploration of secure, scalable, standards-based data exchange that improves the accuracy, timeliness, utility, and responsible stewardship of health information. Intermediaries can connect fragmented systems, support consistent reporting, and enable valuable information to flow back to clinicians and communities. They must, however, complement, not replace, the legal responsibilities and operational capabilities of the nation's federated public health system. The framework should avoid assuming that more centralized retention or broader access to identifiable information always advances public health.

Our recommendations are grounded in AMIA's Public Policy Principles and Policy Positions, especially HIT Data Standards & Interoperability, Population & Public Health, Workforce & Education, Health Data Privacy, Health Information Technology Safety, Artificial Intelligence Principles for Healthcare, Patient Empowerment, and Health and Healthcare Equity. We emphasize evidence-based interoperability, the accurate transmission and interpretation of data, reduced burden on providers and public health personnel, appropriate governance and public trust, and measurable improvements in patient and community health.[1,2]

AMIA offers the following question-by-question recommendations on definitions, standards and technical capabilities, governance, implementation, and dynamic evaluation. We do not address questions focused on financing and payment models.

A. Definition of Public Health Data Intermediary

Question II.A-1: How does this definition of "public health data intermediary" align or conflict with other established definitions, or on-the ground experiences, used across public health and health IT, and what changes would improve distinction or alignment?

AMIA generally supports CDC's proposed definition of a public health data intermediary because it recognizes trusted stewardship, secure and standards-based exchange, protection of privacy and

confidentiality, reduced connectivity burden, and improvements in the quality, timeliness, and usefulness of data. CDC should clarify that this is a functional definition, rather than a requirement that an entity be dedicated exclusively to public health. Health information exchanges (HIEs), health data utilities (HDUs), Qualified Health Information Networks (QHINs), the Association of Public Health Laboratories (APHL) Informatics Messaging Services (AIMS) platform, and other governed services may support public health to different degrees. They should not be treated as interchangeable, and the lack of an intermediary in some jurisdictions should not exclude those jurisdictions from public health exchange.[1]

The definition should identify optional capabilities such as master data management, master patient/person indexes, record matching and deduplication, terminology mapping, validation, enrichment, closed-loop referrals, analytic services, and community information exchange. CDC should distinguish basic transmission and routing from the more consequential functions of retaining, linking, repurposing, or analyzing identifiable data. An intermediary should exercise only the authority lawfully delegated to it. Shared intermediary services should strengthen, not replace, the foundational roles of state, tribal, local, territorial, and federal public health authorities within the nation's federated public health system.

B. Standards and Technical Capabilities

Question II.B-1: Which public health data capabilities, functions, and data sources (e.g., clinical, laboratory, claims, pharmacy, schools, social services) are data intermediaries currently supporting or well positioned to potentially support in the future? For which public health use cases do data intermediaries offer meaningful advantages over direct data exchange or other approaches? Where might the use of data intermediaries add unnecessary cost, complexity, latency, governance burden, or introduce risk? In your response, consider intermediary type, required technical and operational capabilities, and interoperability challenges, informed by: Public Health Data Modernization in Practice: Identification of Core Data Capabilities and Functions.

Intermediaries can support electronic laboratory reporting (ELR), electronic case reporting (eCR), syndromic surveillance, immunization information systems, cancer registries, prescription drug monitoring programs (PDMPs), and other established public health workflows with the use of national standards like HL7 and NCPDP for interoperability, ensuring data privacy and security. They may also assist with vital records, newborn screening, emergency medical services, maternal and child health, chronic disease surveillance, and appropriate exchanges with community-based organizations. Common transport, routing, terminology, and validation services can reduce duplicative point-to-point connections while increasing consistency across healthcare and public health systems. Public health-specific shared infrastructure such as APHL AIMS demonstrates the value of reusable services for appropriate reporting and routing.[1]

CDC should assess the value of an intermediary against direct exchange for each use case, including potential latency, transformation errors, failures in record matching, single points of operational failure, access-control weaknesses, and greater concentration of sensitive data. HIEs that primarily transmit messages differ materially from HDUs or other services that retain and link datasets. Central storage can enable longitudinal surveillance and analysis, but it also raises breach, misuse, liability, and public-trust risks, especially where legal protections or institutional trust are uncertain. CDC should favor data minimization, distributed or federated analysis when feasible, purpose-limited access, explicit retention and

deletion rules, and separate governance for repository functions. An intermediary should not collect identifiable information merely because it is technically able to do so.

Question II.B-2: With the proposed layered approach, which capabilities and standards should sit in the universal baseline versus service-specific or use-case-specific profiles—for example: data quality/provenance (terminology normalization, record matching, longitudinal reconciliation, preservation of source values and transformation rules); exchange/routing (push/query/subscribe, bulk transfer, acknowledgments, jurisdiction-aware routing); security/trust (authentication, authorization, consent enforcement, auditability, incident response); and operational reliability (availability, latency, error rates, incident communication)? Please be specific about minimum requirements.

AMIA supports a layered approach with a clearly defined universal baseline. Every intermediary serving public health should demonstrate applicable national interoperability standards; secure authentication and authorization; encryption; documented data flows; jurisdiction-aware routing; transmission acknowledgments and error handling; availability and incident communication; basic provenance and integrity safeguards; audit logs; and documented procedures to protect privacy and confidentiality. Relevant standards include HL7 v2, HL7 FHIR, nationally recognized code systems such as LOINC and SNOMED CT, and applicable public health implementation guides. The baseline should support integration with certified health IT where relevant, while remaining technologically neutral. Routine transmission should not imply an obligation to store identifiable data. We see this as the floor or basic exchange capabilities only, no repository features. It would therefore need to support exchange/routing, security/trust and operational reliability. This would include supporting APIs that match ONC regulations for CEHRT to ensure ease of interoperability with clinical partners. It would also serve to help exchange data between STLTs and STLTs with the CDC.

Service-specific profiles should contain higher requirements for terminology normalization, conversion across standards, validation of structure and content, master data management, record linkage, master patient/person indexes, deduplication, and enrichment. Deduplication deserves explicit mention: the same case or event may be reported by laboratories, hospitals, and other sources, creating duplicate case investigations or inflated surveillance counts. Validation should distinguish exact duplicate messages from clinically related but nonidentical events, report false matches and missed matches, preserve original source values, and make matching and transformation decisions reproducible and reviewable. Separate, more stringent controls should apply to any repository, longitudinal reconciliation, or analytic use, including justification for storage, access, retention, redisclosure, and breach response. This could also aid in converting/transforming messages between standards (example: HL7 V2 to HL7 FHIR). It could also include data enrichment services to help fill in missing demographic or clinical information.

Public health use-case profiles should then specify reporting mandates, data elements, timeliness expectations, bidirectional functions, and workflow requirements for ELR, eCR, immunization exchange, syndromic surveillance, and other defined purposes. CDC should develop these profiles with the affected public health authorities, laboratories, clinical users, and standards bodies, recognizing that one technical architecture will not be suitable for every jurisdiction or use case.

Question II.B-3: How should data intermediaries be assessed to determine whether they meet applicable capability, standards, performance expectations, security and data protection, and assessment of data

quality? What standardized metrics, evidence, and testing approaches (e.g., conformance testing, certification, validation services) should be used, including to assess onboarding efficiency, scalability, and reach? What existing tools, programs, or approaches could be leveraged?

CDC should recognize existing rigorous frameworks and avoid duplicating assessments unnecessarily. The TEFCA QHIN designation process, relevant Medicaid enterprise system assessment approaches, and the Consortium for State and Regional Interoperability (CSRI) HDU Capability Model are useful inputs. However, a QHIN designation or another assessment should provide evidence toward applicable expectations, not automatic exemption from public health-specific conformance, reliability, governance, or data-quality testing. The CSRI model's focus on distinct stakeholder domains, including public health, can facilitate comparable assessments across intermediary types.[3,4,13]

CDC should require objective evidence from production-like test cases, not self-attestation alone. Assessment measures should include conformance with implementation guides, completeness of transmitted records, clinical and semantic fidelity, accuracy of jurisdictional routing, acknowledgments, duplicate and linkage error rates, timely delivery, uptime, recovery from outages, onboarding time, accessible interfaces, and penetration and incident-response testing commensurate with risk. Data integrity should be measured end to end, from source to recipient: successful transmission is not sufficient if information is altered, omitted, misclassified, or unusable. Clearly assigned operational accountability, privacy and security assessments, and documented corrective actions should be expected for high-impact services. CDC may draw on NIST's Cybersecurity Framework 2.0 (2024) as a complementary cybersecurity risk-management resource.[8]

Question II.B-4: How can a maturity model be useful for advancing data intermediary capabilities over time? If used, in what ways should a maturity model distinguish progression from minimum viable participation to repeatable production and advanced or adaptive capabilities? What capabilities or performance thresholds should characterize each maturity level, and what evidence, including attestation methods, should be required for progression?

AMIA supports a maturity framework that distinguishes safe minimum participation, repeatable production performance, and advanced or adaptive services. CDC should consider CSRI's HDU Capability Model, introduced in October 2025 and updated in May 2026. It evaluates shared capabilities and stakeholder-specific functions for providers, payers, public health, researchers, and patients, and identifies Emerging, Foundational, Advanced, and Aspirational levels. CSRI reported its first member self-assessments in September 2026; that recent experience offers an opportunity to learn about scoring consistency and gaps before applying the model more broadly.[3,4]

CDC should work with CSRI, Civitas Networks for Health, public health jurisdictions, and independent evaluators to refine an interoperable public health capability profile and associated evidence requirements. Graduation between levels should rely on verifiable performance, including stable production exchange, data quality, resilience, user experience, documented governance, and demonstrated value for public health. Requirements should be dated, version-controlled, periodically reviewed, and revised when technical standards, risks, or public health needs change. A maturity model should guide improvement, not become a rigid one-size-fits-all condition that disadvantages smaller or specialized intermediaries.

Question II.B-5: How might artificial intelligence (AI) capabilities affect data intermediaries' technical, governance, and operational roles—including accelerating, replacing, or distributing functions?

AI can improve labor-intensive functions such as mapping local terminology to standard code sets (e.g. LOINC and SNOMED CT), validating HL7 v2 and FHIR messages, identifying anomalous reporting patterns, deduplicating records, and analyzing free-text reports. Used appropriately, these capabilities could improve consistency and reduce manual review. However, these potential benefits should be demonstrated in the intended operational setting rather than presumed. AI cannot assume responsibility for legal authority, permitted data use, public health judgments, or institutional accountability.[2,9]

CDC should explicitly address automation bias, incorrect inferred values, differential performance across patient populations, opaque model changes, cybersecurity vulnerabilities, adversarial manipulation, and the risk that AI-generated errors or alerts shift rather than reduce clinicians' or public health personnel's workload. Intermediaries using AI should preserve original values, label inferred or altered information, record model and rule versions, retain auditable transformation histories, and support meaningful explanation and reproduction of results. Human review should be required for high-impact determinations, such as case classification, significant identity matches, and actions that could affect individual rights or public health interventions. Interfaces should make uncertainty and override procedures understandable.

CDC should encourage predeployment validation against representative reference datasets, ongoing assessment for model drift and disparate performance, incident reporting, cybersecurity testing, and human-in-the-loop verification proportionate to risk. Access to patient-level information for AI training must be separately authorized, transparently governed, and protected against unauthorized reuse and re-identification, including respect for tribal data sovereignty. NIST's AI Risk Management Framework (2023) offers an appropriate starting point for risk management but should be adapted to specific public health workflows.[9]

D. Governance

Question II.D-1: What governance and accountability expectations should apply to data intermediaries, and should these vary based on the functions performed, the data handled, the entities/communities served, or the jurisdiction's laws and authorities?

AMIA supports a common governance floor for transparent data stewardship, privacy, security, accountability, auditability, and incident response, supplemented by requirements proportionate to the functions performed and the data handled. Governance should identify the entity with authority to approve each use case, the intermediary's delegated responsibilities, its permitted uses and retention periods, procedures for resolving conflicts, and accountability for failures or unauthorized disclosures.

State- and jurisdiction-based governance can be especially responsive to local public health duties and statutory requirements; it should nevertheless operate within compatible national interoperability standards. A public health authority should have meaningful participation in governing services on which it relies, and tribal sovereignty must be respected. Intermediaries carrying out long-term storage, linkage, or sensitive analytics need additional scrutiny. Written agreements and independent assessments should address breach notification, contingency planning, legal responsibility, and organizational readiness. The

authority and duties of public health agencies must not be displaced by technology vendors or other intermediaries.

Question II.D-2: What safeguards would ensure transparent access to data intermediary services and prevent conflicts of interest, biased routing, vendor lock-in, proprietary dependencies, or market concentration—including across jurisdictions with differing legal requirements?

CDC should recommend transparent, nondiscriminatory participation criteria, published routing and access policies, disclosure of material conflicts of interest, and enforceable mechanisms for oversight and appeal. Intermediaries should not use their position to favor selected users, obscure data access decisions, or create proprietary dependencies. Standards-based portability, documented interfaces, provenance, and continuity or exit planning can limit lock-in while allowing jurisdictions to leverage valuable existing networks.

AMIA supports reusable shared infrastructure but cautions against mandating a single exclusive state or national intermediary. The appropriate approach may be a state-governed HIE, a regional HDU, a QHIN-connected network, or specialized public health services such as APHL AIMS, depending on jurisdictional needs and responsibilities. A shared governance body should include public health leadership, clinical and laboratory partners, informatics experts, and other appropriate stakeholders and should document how decisions about new data uses and capabilities are made.

Question II.D-3: What requirements should govern a data intermediary's authority to receive, access, route, transform, enrich, or disclose public health data, including delegated authority, reciprocal exchange, and compliance with jurisdiction-specific laws?

An intermediary's authority must be grounded in applicable law, delegated functions, and documented permissible purposes; it must not exceed the authority of the entities on whose behalf it operates. CDC should acknowledge that "public health data" is not a uniformly defined legal category across jurisdictions and that federal, state, tribal, local, and territorial reporting and privacy requirements may differ. The existence of technical access should never be treated as sufficient authority to collect, retain, redistribute, or combine information.

Governance agreements should specify the data categories and uses authorized; limits on onward disclosure, reuse, and model training; controls on identity linkage and enrichment; and safeguards for information derived from patient surveys or social and environmental circumstances. CDC should explicitly distinguish information required for legally authorized public health reporting from patient-reported or community-based information gathered for a different purpose. Sensitive social-needs data should not automatically become available for broadly defined surveillance or other secondary uses. Where new access is contemplated, CDC should require a clear use-case justification, proportional data collection, transparency, community engagement, and appropriate legal and technical protections.

Question II.D-4: What roles should CDC, other federal agencies, state, tribal, local, and territorial (STLT) public health authorities, data intermediary governing bodies, participants, and other relevant entities play in oversight and accountability? How should these roles be coordinated, and what monitoring, audit, corrective-action, suspension, sanction, or termination mechanisms are appropriate?

Intermediary governing bodies should be structured to provide meaningful voice to the state, tribal, local, and territorial public health authorities that depend on the service, alongside healthcare organizations,

laboratories, informatics experts, and other affected partners. The governing body should set priorities, review new uses, establish operational requirements, approve material changes, and oversee independent audits. It should have defined mechanisms for corrective action, suspension, termination, and continuity of essential public health exchange.

For widely used shared public health services, including APHL AIMS, CDC should work with STLT partners and existing service stewards to clarify governance responsibilities and ensure broad jurisdictional participation. CDC and other public health stakeholders should also engage appropriately with TEFCA governance, including development of public health-specific operating procedures and clear testing of compliance with jurisdictional restrictions. Oversight should verify that audit trails, incident investigations, and security controls work in practice, rather than assuming that contractual assurances alone are sufficient.

Question II.D-5: How should governance accommodate jurisdictional differences in law, reporting mandates, privacy, consent, data use agreements, and public health authority while minimizing administrative, technical, and financial burden and supporting equitable participation?

CDC should identify a national baseline of security, transparency, data quality, and interoperability expectations while preserving legitimate state, tribal, local, and territorial differences in authority, reporting mandates, privacy law, and consent requirements. Jurisdictions should be involved in establishing common requirements and documenting permitted variations, similar to collaborative processes used to reconcile public health case definitions. Intermediaries should provide auditable, technically enforceable jurisdiction-aware rules and practical procedures for documenting applicable restrictions.

National exchange agreements cannot, on their own, resolve every conflict in local law or establish trust. CDC should therefore encourage clear governance, operational testing, transparent decisions about data access, and accessible guidance for smaller jurisdictions and tribal entities. Privacy, security, and equitable participation should be evaluated together: systems are not successful if marginalized populations are underrepresented, their information is used in ways that undermine trust, or community partners are excluded from governance.

E. Implementation

Question II.E-1: What tools, templates, or guidance (e.g., implementation playbooks, procurement language, data use/service-level agreement templates, security checklists, evaluation tools, governance models) do public health agencies need to evaluate, select, implement, and oversee data intermediary partnerships, and their associated outcomes?

CDC should provide a coordinated implementation toolkit that public health agencies can adapt to evaluate, select, implement, and oversee intermediary partnerships. It should include use-case playbooks; relevant implementation guides; templates for data use agreements and governing-body charters; model procurement and service requirements; sample agency-wide intermediary policies; privacy and security review checklists; data-quality test plans; operational escalation procedures; vendor exit and continuity plans; and example measures of implementation success. Templates should identify when an intermediary only transports data and when additional requirements apply for repository, deduplication, identity linkage, enrichment, or analytics functions.

Rather than develop resources from the beginning, CDC should use and cross-reference existing materials, including Civitas Networks for Health and the Maryland Health Care Commission's Health Data Utility Framework—A Guide to Implementation (March 2023), the CSRI HDU Capability Model (released October 2025; updated May 2026), and operational models such as CRISP Shared Services, which supports reusable infrastructure across jurisdictions. CDC should also draw on relevant TEFCA selection and participation guidance and experience from established HIEs and HDUs. These are implementation resources, not universal certification substitutes: each should be evaluated for fit with specific public health workflows.[3–7]

AMIA recommends that CDC encourage each public health agency to establish a leadership-approved, organization-wide policy for assessing and using intermediaries. Such policies can reduce fragmented decisions across program silos, define the role of the chief informatics or technology officer, set common standards and security expectations, and create consistent exceptions and review procedures. CDC could collaborate with CSRI and Civitas to maintain an implementation resource library and common testing framework. Each template should identify its issue date, version, last review date, applicable standards, and review trigger so users can recognize outdated guidance without imposing arbitrary expiration periods.

Question II.E-2: What barriers (e.g., workforce, funding, procurement, legal authority, governance, technical infrastructure, trust, sustainability, jurisdictional variation)—limit STLT public health agency readiness to use data intermediary services, and what support would address them? How should implementation build on existing investments and support coexistence, migration, or transition without unnecessarily replacing already functioning infrastructure? Where relevant, note differences by data intermediary type.

Barriers include uneven public health informatics workforce capacity, limited technical infrastructure, fragmented agency program processes, inconsistent standards adoption, differences in jurisdictional authority, lengthy procurement and contracting processes, lack of confidence in data stewardship, and inadequate access to qualified technical assistance. Barriers also differ among intermediary types: a transport-only HIE has different readiness requirements from an HDU hosting longitudinal repositories, while QHIN-related exchange may raise additional questions about public health queries, participation obligations, and the applicability of jurisdiction-specific rules. These barriers should not be treated solely as technology problems.

CDC should provide high-level implementation guidance anchored in AMIA's principles on HIT Data Standards & Interoperability, Workforce & Education, Health Data Privacy, Population & Public Health, and Health and Healthcare Equity. Recommended approaches include readiness assessments, workforce competencies and training, legal and data-governance guidance, standards-based onboarding, leadership-approved policies, and a structured process for identifying when existing investments can be reused. The Civitas implementation framework and the CSRI capability model can help agencies distinguish basic infrastructure and governance deficiencies from gaps in advanced services.[2–5]

For established systems, CDC should encourage phased transition plans, parallel testing, continuity safeguards, and interoperability among functioning HIEs, HDUs, public health-specific platforms, and networks participating in TEFCA. The objective should be less duplicative work, fewer manual reporting steps, and more reliable data, not migration for its own sake. CDC should incorporate smaller, rural, tribal, and safety-net partners into implementation planning and ensure that clinicians and public health staff do

not inherit additional data-entry tasks. No single delivery model should be presumed appropriate across every state or jurisdiction.

Question II.E-3: What approaches should CDC consider to test, learn from, and scale promising intermediary models or capabilities for public health purposes? How can pilots, demonstrations, learning collaboratives, phased implementation, or other approaches build evidence and trust while informing decisions about whether, when, and how to scale?

CDC should support phased demonstrations and learning collaboratives using explicit, testable hypotheses and comparisons against existing practice. AMIA recommends three stages: (1) establish baseline accuracy, timeliness, user burden, privacy risks, and implementation readiness; (2) conduct small, well-monitored demonstrations with independent validation and a process for resolving unexpected harms; and (3) expand only after the model demonstrates reliable performance and practical benefits across different settings. Learning collaboratives should include STLT public health agencies, hospitals, clinicians, laboratories, community organizations, informatics researchers, and resource-constrained participants.

Priority demonstrations should include eCR, ELR, immunization information exchange, cross-source deduplication, terminology validation, and reciprocal data returns to clinical workflows. CDC can draw lessons from its Implementation Center Program, including Wave 2 use cases in chronic disease, maternal and child health, cancer reporting, and biothreat detection, as well as experiences with APHL AIMS and state/regional HDUs. The Civitas framework and CSRI assessments offer complementary structures for evaluating organizational readiness and capabilities.[3–5,10]

CDC should also test carefully scoped approaches to patient-reported information and social determinants of health (SDOH) or other social-needs data, including whether these data improve understanding of patient outcomes and quality of care. Such demonstrations must evaluate representativeness, patient understanding, accuracy, missingness, potential stigma, privacy, confidentiality, authorized use, and whether information could be repurposed for unwanted surveillance or administrative action. More collection should not be the default outcome: privacy-preserving aggregation, federated approaches, and noncollection should remain options. Pilot results should be published with the dates, population, implementation conditions, and limits on generalizability.

Question II.E-4: Where do public health needs and capabilities align with those of healthcare providers, payers, laboratories, community organizations, and other partners? What data, information, services, or capabilities could public health provide to partners (e.g., providers) through intermediaries to create shared value and strengthen reciprocal exchange? What collaboration approaches could enable this value, and what constraints, tensions, or tradeoffs should be considered?

Public health agencies should be active participants in reciprocal exchange, not merely recipients of data from healthcare organizations. Where authorized and appropriate, they can offer immunization histories and forecasting, newborn screening and other laboratory results, vital-record information, PDMP information for authorized users, population-level surveillance trends, emergency preparedness indicators, and timely public health alerts. Clinical and community partners may also benefit from closed-loop referrals and relevant screening or social-services information when sharing is legally permitted and consistent with the individual's expectations. These functions can make participation valuable to healthcare providers and

patients, provided the returned information is accurate, timely, clinically meaningful, and accessible in the existing workflow.

Intermediaries should support standards-based EHR integration so that clinical staff do not have to search several separate portals, re-enter results, or correct duplicate and conflicting records. CDC should work with clinical partners to measure the accuracy of data transmitted in both directions, the extent of unnecessary or repeated reporting, the time required to retrieve and reconcile information, and whether returned information improves care and public health response. Shared governance should include clinicians, laboratories, public health agencies, and community representatives in prioritizing the information that is genuinely useful.

Reciprocal exchange must be purpose-limited: not all public health datasets should be redistributed to all healthcare partners. Sensitive data, especially patient-reported social needs and other contextual information, require clear legal authority, need-to-know controls, data minimization, and safeguards against misuse. CDC should encourage informed community engagement and public communication about how information is exchanged and used.

Question II.E-5: Where can CDC add the greatest value in strengthening the data intermediary ecosystem, and through what role(s)—for example, as a convener, funder, purchaser, technical assistance provider, standards advocate, evaluator, or facilitator of shared infrastructure? Where should CDC instead leverage, align with, or defer to existing public- and private-sector efforts?

CDC is well positioned to serve as a convener, standards advocate, source of technical assistance, evaluator, and facilitator of compatible public health data-exchange practices. CDC should coordinate closely with ONC, CMS, STLT public health agencies, standards development organizations, existing intermediary services, laboratories, healthcare organizations, and the research community. Coordination should align public health reporting with relevant EHR certification requirements, quality-measurement standards where useful, TEFCA processes, and initiatives such as the HL7 Helios FHIR Accelerator. AMIA can contribute as a neutral, multidisciplinary convener of clinical and public health informatics stakeholders.[13,14]

CDC should build on trusted capabilities, including APHL AIMS, existing state and regional HIEs and HDUs, CRISP Shared Services, and QHIN-related exchange, rather than establish duplicative pathways without demonstrated added value. The agency should develop clear, collaboratively governed guidance, convene learning collaboratives, support rigorous evaluation and dissemination, and give STLT partners meaningful influence over the design of services on which they depend. CDC should also consider complementary input developed by the Joint Public Health Informatics Taskforce (JPHIT) and public health laboratory stakeholders; AMIA does not presume to speak for those groups.[11]

Importantly, CDC's role as a national coordinator should not be equated with a blanket need to gather or retain identifiable patient information centrally. Before creating a new federal collection or access pathway, CDC should articulate its statutory authority, specific public health use, minimum required data, access and retention controls, independent oversight, and privacy-preserving alternatives. The ultimate measure of success is improved patient and community health, not the volume of data held by an agency or transmitted through an intermediary.

F. Dynamic Evaluation

Question II.F-1: Where can CDC add the greatest value as an evaluator (e.g., in providing guidance on evaluating pilots or implementation models, synthesizing evaluation evidence across settings, or evaluating the strategic outcomes and value of the broader intermediary framework)?

CDC should develop a consistent but adaptable evaluation structure that allows comparisons across intermediary types, public health use cases, and jurisdictions. It can establish shared definitions and measurement methods, collect implementation lessons, examine unintended effects, and synthesize evidence from pilots and routine operations. CDC should distinguish performance attributable to the intermediary from broader changes in underlying data systems, staffing, reporting law, or public health practice.

AMIA recommends independent evaluations by academic institutions or other qualified evaluators, working with STLT agencies and other participating organizations. Transparent publication of both successful and unsuccessful implementations strengthens public health informatics as a science and helps avoid repetition of ineffective approaches. Reporting should include baseline conditions, implementation dates, relevant standards and framework versions, measures collected, methods, limitations, and whether findings generalize to different intermediary types. CDC's Implementation Center demonstrations and work by Civitas, CSRI, and public health organizations can supply useful opportunities for such evaluations.[3–5,10]

Question II.F-2: What frameworks, benchmarks, and measures should CDC use to evaluate the intermediary framework, including impacts on workflows, workforce burden, user experience, data usability, situational awareness, and response capacity? What data sources and methods could support feasible measurement and assess the contribution of intermediary-enabled exchange to observed changes and, where feasible, support causal attribution?

AMIA recommends a balanced set of benchmarks that measures more than connectivity or exchange volume. First, technical reliability should capture availability, transaction success, routing accuracy, latency, acknowledgments, incident recovery, and continuity.

Second, data quality should assess whether complete, correct information reaches the intended recipient with original meaning preserved: source-to-destination field agreement, terminology accuracy, missingness, patient-matching sensitivity and specificity, duplication rates, and traceable transformations.

Third, operational burden should measure the time and effort healthcare professionals, laboratories, and public health staff spend entering, correcting, reconciling, and locating information; repeat reporting; the number of disconnected portals; and user experience. A successful intermediary should improve transmission accuracy and reduce provider burden, not merely increase throughput.

Fourth, privacy and security should be evaluated through access-control testing, adherence to purpose limitations, breach and near-miss reports, incident response, audit-log effectiveness, unnecessary retention, and public trust.

Fifth, equity measures should examine whether smaller, rural, tribal, safety-net, and other historically under-resourced partners can participate, and whether missing or inaccurate data disproportionately affect particular communities.

Sixth, reciprocal exchange should measure the usability and timeliness of immunization, PDMP, laboratory, or public health information returned to clinicians when lawfully authorized.

Seventh, public health impact should assess timelier detection and investigation, more useful situational awareness, and improvements in community and patient outcomes where credible attribution is possible.

One suggestion would be to use the evaluation approaches discussed in these articles: "Evaluating Public Health Uses of Health Information Exchange" and "A Framework for evaluating the costs, effort, and value of nationwide health information exchange". CMS also has a new Interoperability Framework as part of their Health Tech Ecosystem - Interoperability Framework. We do encourage HHS collaboration in this space to try and ensure all health ecosystem partners are moving in a coordinated fashion forward.[12,16,17]

CDC should adapt established evaluation approaches, including the peer-reviewed framework for public health uses of HIE (2007), the CSRI HDU Capability Model (2025–2026), the Civitas HDU Framework (2023), and the NIST Cybersecurity Framework 2.0 (2024). Measures of AI-supported operations can additionally draw on the NIST AI Risk Management Framework (2023) and should include auditability, model drift, explainability, unintended errors, and evidence of appropriate human verification. Metrics should use feasible data sources and account for measurement burden and align with the CMS required outcomes and metrics for HIE certification. Phased rollouts, matched comparison sites, time-series analysis, and pre/post testing may support attribution, with explicit acknowledgment of limitations. Every performance measure and technical reference should have a date and version, and CDC should periodically review its validity as technologies and use cases evolve.[3–5,8,9,12,18]

Conclusion

AMIA appreciates CDC's efforts to develop a more effective and accountable public health data-intermediary ecosystem. We support a flexible, layered framework that builds on existing infrastructure and widely adopted standards; protects individual privacy, confidentiality, and jurisdictional authority; and requires meaningful evidence that exchanged data are accurate, useful, and secure. The framework should distinguish transport from retention and analytics, recognize deduplication and data provenance as important capabilities, and incorporate risk-proportionate oversight for AI-enabled functions.

CDC should also make implementation and evaluation central to its approach. Reusable guidance, agency-wide governance policies, phased demonstrations, independent assessment, reliable bidirectional exchange, and measured reductions in administrative burden can help translate technical capabilities into better outcomes. CDC should engage public health authorities, clinical and laboratory partners, communities, and informatics professionals in ongoing development and regularly revisit the guidance as standards and risks change.

AMIA looks forward to continued collaboration with CDC and its partners. Thank you for considering these comments. Please contact Tayler Williams, Senior Manager of Public Policy, at twilliams@amia.org with any questions.

Sincerely,

Eileen Koski

Eileen Koski
Chair, AMIA Public Policy Committee

References

[1] Centers for Disease Control and Prevention. Data Intermediaries and Approaches to Strengthen Public Health Data Exchange. Request for Information. 91 FR 59777. September 21, 2026. https://www.federalregister.gov/documents/2026/09/21/2026-19271/data-intermediaries-and-approaches-to-strengthen-public-health-data-exchange

[2] American Medical Informatics Association. AMIA Public Policy Principles and Policy Positions: 2024–2029 Priorities. 2025 version. https://brand.amia.org/m/7094a39156542fdf/original/AMIA-Public-Policy-Principles-2025.pdf

[3] Consortium for State and Regional Interoperability. Health Data Utility Capability Model. Released October 28, 2025; updated May 12, 2026. https://thecsri.org/the-csri-health-data-utility-capability-model/

[4] Consortium for State and Regional Interoperability. Completion of First Self-Assessments Using the Health Data Utility Capability Model. September 22, 2026. https://thecsri.org/news/press-release/the-consortium-for-state-and-regional-interoperability-csri-announces-completion-of-first-self-assessments-using-the-health-data-utility-capability-model/

[5] Civitas Networks for Health and Maryland Health Care Commission. Health Data Utility Framework—A Guide to Implementation. March 2023. https://civitasforhealth.org/hduframework/

[6] CRISP Shared Services. Organizational website and implementation examples. https://www.crispsharedservices.org/

[7] Florida Health Information Exchange. Who Is CRISP Shared Services? March 26, 2026. https://www.flhie.org/faq/who-is-crisp-shared-services/

[8] National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0. February 26, 2024. https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20

[9] National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). January 26, 2023. https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10

[10] Public Health Infrastructure Grant. Implementation Centers, Wave 2. 2026 program description. https://www.phinfrastructure.org/implementation-centers/wave-2/

[11] Association of Public Health Laboratories. CDC Intermediary RFI—Policy Engagement. Updated October 12, 2026 (records APHL's coordination with the Joint Public Health Informatics Taskforce). https://aphlinformatics.atlassian.net/wiki/spaces/PE/pages/5474582560/CDC+Intermediary+RFI

[12] Shapiro JS, et al. Evaluating Public Health Uses of Health Information Exchange. 2007. https://pmc.ncbi.nlm.nih.gov/articles/PMC2137930/

[13] The Sequoia Project. QHIN Application, Onboarding, and Designation Process. ONC TEFCA Recognized Coordinating Entity. https://rce.sequoiaproject.org/qhin-process/

[14] Health Level Seven International (HL7). Helios FHIR Accelerator for Public Health Home. HL7 Confluence. https://confluence.hl7.org/spaces/PH/pages/77367966/Helios+FHIR+Accelerator+for+Public+Health+Home

[15] Office of the National Coordinator for Health Information Technology (ONC). Certification Program Regulations. Last updated October 28, 2026. https://healthit.gov/certification-health-it/certification-program-regulations/

[16] Dixon BE, Zafar A, Overhage JM. A Framework for Evaluating the Costs, Effort, and Value of Nationwide Health Information Exchange. Journal of the American Medical Informatics Association. 2010;17(3):295–301. https://pmc.ncbi.nlm.nih.gov/articles/PMC2995720/

[17] Centers for Medicare & Medicaid Services. Interoperability Framework. CMS Health Technology Ecosystem. Launched July 30, 2025; page last modified November 13, 2026. https://www.cms.gov/initiatives/health-technology-ecosystem/overview/interoperability-framework

[18] Centers for Medicare & Medicaid Services. MES Certification Repository: Health Information Exchange (HIE). Outcomes and Metrics. https://cmsgov.github.io/CMCS-DSG-DSS-Certification/Outcomes%20and%20Metrics/Health%20Information%20Exchange%20(HIE)/