HTI-5 Proposed Rule:

What It Means for Healthcare Organizations Using Certified Health IT

February 23, 2026

RISING T1DE ALLIANCE

www.risingt1dealliance.org • risingt1dealliance@luriechildrens.org

Table of Contents

To cite this report:
Espinoza J; Rising T1DE Alliance. *HTI-5 Proposed Rule: What It Means for Healthcare Organizations Using Certified Health IT*. White paper. Published February 10, 2026. https://risingt1dealliance.org/

Executive Summary

HTI-5 is a deregulatory proposal that would substantially narrow ONC's Health IT Certification Program by removing many certification criteria, especially in privacy/security and process/design requirements, while reinforcing a long-term shift toward FHIR® API-based interoperability as the primary mechanism for scalable access, exchange, and use of electronic health information (EHI). At the same time, HTI-5 proposes targeted updates to information blocking (45 CFR Part 171), including clarifications that "access" and "use" of EHI include automated means (including autonomous AI systems), and proposals affecting the structure of exceptions (including TEFCA-specific provisions). For healthcare organizations, the most important impact is downstream: certification may become limited in scope. As a result, there may be greater variability in how vendors implement solutions. Organizations should plan to address security controls, accessibility requirements, auditability, and app enablement through contracting processes and local governance rather than relying on certification alone.

High-level actions for healthcare leaders

ACT:

- Treat this as a contracting/procurement issue, not just a "vendor compliance" issue. If certification becomes narrower in scope, identify what you still require (security controls, auditability, accessibility, decision-support documentation) and put it into contracts/SOWs rather than assuming certification covers it.
- Get a written HTI-5 impact statement from your EHR and key certified module vendors. Ask what they plan to deprecate, keep "as standard," or move into optional modules; request a timeline and a list of hospital-facing changes (upgrades, config, workflows).
- Stand up (or refresh) an "API/app enablement governance playbook." HTI-5 emphasizes automated access/use. Align security, privacy, CMIO, and IT ops on app onboarding, scopes, throttling, auditing, incident response, and denial documentation.
- Define your minimum AI/CDS governance artifacts now (even if certification rolls back). Decide what you will require for predictive tools (intended use, limitations, validation population, monitoring plan, escalation path), and make it a standard intake requirement for any vendor or internal deployment.

MONITOR:

- Final scope/timing of certification removals and revisions. Some items have delayed effective dates; ensure upgrade planning and procurement assumptions align to the final rule text.
- Information blocking definition/exceptions changes and enforcement posture. Watch how "automation/AI-enabled access and use" is treated in final language and related guidance, and how exception revisions affect your operational "no/slow" decisions.
- TEFCA implications (especially the proposed removal of the TEFCA Manner Exception). Track whether "TEFCA-only" responses become harder to justify and what that means for your exchange strategy and partner expectations.
- Market behavior: where vendors continue strong controls vs where they cut back. Expect interoperability capabilities to improve faster than governance/documentation unless buyers demand both; monitor early signals from your vendor's roadmap and peer institutions.

BOTTOM LINE:

- Opportunity: Faster, more scalable interoperability if the ecosystem truly shifts to modern APIs and measurable exchange.
- Risk: If certification provides fewer assurances healthcare organizations may need to take on more responsibility through governance, evidence requirements, monitoring, and contractual safeguards

1. Introduction

The Health Data, Technology, and Interoperability (HTI-5) Proposed Rule is best understood as a policy "reset" that would narrow the scope of federal certification while emphasizing API-enabled interoperability and stronger expectations for access to electronic health information. While the ONC certification program is voluntary and primarily regulates developers, healthcare organizations (HCOs) depend on certified capabilities for patient access, interoperability, quality reporting, and day-to-day operations, so changes in certification scope can meaningfully alter what HCOs can assume is "standard" in their EHR environment. This memo is written for hospital leadership and highlights where HTI-5 changes the regulatory baseline versus where it primarily shifts market incentives and operational expectations.

Why this matters to the Rising T1DE Alliance (RTA): The RTA is focused on ensuring that diabetes data are available, usable, and actionable for clinicians so patients can receive high-quality, data-driven care. Because HTI-5 emphasizes API-based interoperability and real-world access to electronic health information, its direction could materially influence how easily diabetes data flow across systems and into clinical workflows.

2. What HTI-5 Is and Why ASTP/ONC Issued It

HTI-5 ("*Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity*") is a proposed rule that would revise 45 CFR Part 170 (ONC Health IT Certification Program) and 45 CFR Part 171 ("Information Blocking"). ASTP/ONC frames HTI-5 as part of a broader deregulatory initiative intended to reduce administrative burdens on providers and developers, improve access to electronic health information (EHI), and promote competition in the certified health IT market. ASTP/ONC's press release describes three "core goals": (1) streamline certification by removing redundant requirements (reducing developer burden), (2) update information blocking regulations to promote EHI access/exchange/use (so patient access is not blocked), and (3) advance a FHIR-based API foundation to promote AI-enabled interoperability solutions.

3. Big Changes at a Glance

Topic	What Changes?	Who is Directly Regulated?	What HCOs Should Expect
Certification Scope	Proposed to remove over half of certification criteria and revise others; "reset" future scope toward standards-based APIs/FHIR and AI-enabled interoperability	Health IT developers (Part 170 program)	Less "built-in" assurance that certain security/design/process capabilities remain present by virtue of certification; more reliance on contracting and local governance
Privacy/Security Criteria	Proposed removal of many privacy/security certification criteria (authentication, audit logs, integrity, encryption, etc.)	Health IT developers	HCOs may need to explicitly require these controls in procurement/security addenda even if not required for certification
Patient Access (Portal/VDT)	Proposed revision to VDT criterion to remove a specific accessibility standard reference (WCAG 2.1 Level AA) while retaining a functional requirement	Health IT developers	Patient portal/app access continues, but HCOs may need separate accessibility governance/requirements if they rely on WCAG compliance as a vendor obligation
Public Health Reporting Criteria	Multiple public health-related criteria proposed for removal with transition timing described for some	Health IT developers	Potentially fewer federally required "certified" public health interfaces; HCOs may see changes in vendor roadmaps and optional modules
App/API Access Criteria	Proposed removal (with timing) of "application access" criteria, including patient selection and "all data request"	Health IT developers	Potential changes in how EHRs certify/offer API access capabilities; HCOs may need stronger contracting on app enablement, throttling, and third-party onboarding
Information Blocking	Proposed revisions/removals of definitions and exception conditions; aim to better promote EHI access/exchange/use and strengthen enforceability	Actors subject to Part 171 (including providers in scope)	"Downstream" operational pressure to reduce friction for authorized third-party apps/automation/analytics; revisit policies, app approval and denial rationales, and documentation
"AI-Enabled Future" Framing	Press release emphasizes AI-enabled interoperability via modernized standards/certification; possible rollback of certain AI transparency/ documentation certification requirements	Health IT developers (Part 170) and Part 171 actors	HCOs should plan for more local governance of CDS/AI tool transparency, monitoring, and risk management as certification requirements narrow
Program Administration & Maintenance	Rule includes sections on conditions/maintenance (assurances, APIs, real world testing, attestations, insights) and administrative requirements	Health IT developers; ONC-ACBs	HCOs may still see vendor attestations/real-world testing artifacts, but should not assume prior breadth/format persists

4. Certification Criteria Changes – Part 170

What the proposed rule says

HTI-5 proposes a broad set of changes to the ONC Health IT Certification Program, centered on removing or revising a substantial share of the current certification criteria in 45 CFR 170.315 (and related program elements). In aggregate, the proposal would remove many criteria outright and revise a smaller set, with the heaviest reductions concentrated in privacy/security safeguards, along with removals in several interoperability/exchange and public health reporting areas, and multiple design/process and application access requirements. The revisions that remain generally trend toward "functional" requirements while reducing or removing prescriptive standards references and certain certification-side assurance artifacts. Illustrative examples removals and revisions include:

- Patient demographics and observations (§ 170.315(a)(5)): proposes revision to remove a specific standard reference related to "sex" and require the capability to record patient sex.
- VDT (§ 170.315(e)(1)): proposes revision to remove the requirement to conform with WCAG 2.1 Level AA (certification-side) while keeping a functional patient access approach.
- Electronic case reporting (eCR) (§ 170.315(f)(5)): proposes revision described as "functional only," removing specific standards-based requirements (and reserving the standards-based subsection).
- AUR (§ 170.315(f)(6)): proposes revision described as "functional only" and removing a specific standard reference.
- Transmission to cancer registries (§ 170.315(f)(4)): proposed removal.
- Transmission to public health agencies—health care surveys (§ 170.315(f)(7)): proposed removal.

What it means simply

- Certification would become less prescriptive about how products are designed, documented, tested, and governed in several domains (particularly privacy/security and developer process requirements).
- HCOs should treat "certified" as a narrower assurance: certification may still matter, but it will be less aligned with certain operational expectations HCOs often assume come "standard" with a certified EHR/module.

How it differs from before

Under the current baseline framework (45 CFR 170.315 as of 2/06/2026), HCOs and vendors often rely on certification criteria and ONC test methods as a practical "checklist" of capabilities and compliance artifacts. HTI-5 proposes to remove a material share of that checklist and revise some criteria to be less tied to specific standards.

Downstream implications HCOs may experience

- Procurement & contracting: If a criterion is removed from certification, HCOs that still need the capability (e.g., audit logs, encryption, user authentication patterns, specific public health reporting functions) should contract for it explicitly, rather than assuming certification will compel the vendor to maintain it.
- Upgrade planning: Vendor roadmaps may shift away from certain legacy/document-centric exchange features and toward API-centric interoperability; HCOs should align interoperability strategies to what remains required vs. what becomes optional/market-driven.
- "Certification as a floor": Practically, ONC certification may become more about API baseline interoperability and less about "enterprise-grade" governance/security-by-certification. HCOs will likely need to reinforce governance through local policy, security architecture, and contract terms.

5. Information Blocking Changes – Part 171

What the proposed rule says

HTI-5 proposes revisions to information blocking regulations to better promote EHI access, exchange, and use, including revisions/removals of certain terms/conditions/exceptions to address potential misuse and to strengthen enforceability. The proposed rule also explicitly links these changes to supporting providers' ability to use innovative third-party software with their EHRs and to support access/exchange/use of patients' EHI.

- Definitions: revises § 171.102 "access" and "use" to emphasize they include automated means, "including… autonomous AI systems" (and an alternative proposal to revise "exchange" similarly).
- Infeasibility exception: proposes removing the "third party seeking modification use" condition (§ 171.204(a)(3)), and propose revising or removing the "manner exception exhausted" condition (§ 171.204(a)(4)).
- Manner exception guardrails: proposes revising § 171.301(a) to clarify the manner exception can't be satisfied with contracts that are not market-rate / are adhesion / unconscionable.
- TEFCA: proposes removing the TEFCA Manner Exception (§ 171.403) and removing Subpart D (171.400/171.401/171.403) as unnecessary.
- Public health reporting: Proposed removal of Transmission to cancer registries (§ 170.315(f)(4)), proposed revision to electronic case reporting (§ 170.315(f)(5)) to keep functional requirements but remove standards-based requirements

What it means simply

Even if most HTI-5 changes "directly" regulate developers, the information blocking portion can create real operational pressure on HCOs to:

- Reduce unnecessary friction in patient-authorized third-party app enablement
- Make app access more consistent and predictable
- Document denials/delays carefully under applicable exceptions

How it differs from before

The proposed rule signals continued movement from "traditional" request/response exchange patterns toward more automated access and use of EHI. This increases the likelihood that system design choices (rate limits, app approval workflows, contractual controls, security postures) become information blocking–relevant issues.

Downstream implications HCOs may experience

- App enablement governance becomes a compliance-adjacent topic. decisions about which apps get access, what scopes they get, and how quickly access is provisioned may draw increased scrutiny if access is unreasonably impeded.
- Operational alignment needed across IT security, privacy, compliance, and clinical operations so "safety/security" rationales are consistent, time-limited where appropriate, and tied to documented facts.

6. AI & Decision Support Implications

What the proposed rule says

HTI-5 presents its proposed certification and interoperability changes as supporting an AI-enabled future, emphasizing modernized standards and a refocus on FHIR-based APIs. In Part 171, ONC also proposes to clarify that information blocking concepts apply to automated and AI-enabled activity—not just manual workflows.

- Information blocking (45 CFR Part 171)
  - § 171.102 ("access" and "use"): proposes to revise the definitions to make explicit that "access" to, and "use" of, EHI include automated means, including "without limitation" autonomous AI systems ("agentic AI").
  - § 171.102 ("exchange") request for comment/alternative: solicits comment on revising "exchange" similarly to clarify that automated transmission of EHI is within scope.
- Certification (45 CFR Part 170)
  - § 170.315(a)(9) Clinical decision support (CDS): proposes to remove the CDS certification criterion (effective date of the final rule).
  - § 170.315(b)(11) Decision support interventions (DSI): proposes to revise the DSI criterion, including scaling back certain predictive DSI transparency/governance-adjacent requirements (e.g., proposed removal of requirements related to source attribute support/access/modification and proposed removal of predictive DSI risk management requirements).
  - AI "model cards": the proposed rule states that these DSI revisions would fully remove AI "model card" requirements from the criterion.

What it means simply

HTI-5 is signaling that AI-enabled and automated data flows are now a mainstream part of interoperability policy, and that information blocking analysis is not limited to human-driven requests. At the same time, HTI-5 would make certification less prescriptive about decision support documentation and governance artifacts by removing the CDS criterion and narrowing DSI requirements, including eliminating model card requirements.

Practically speaking, HCOs should not assume that "certified" decision support comes with standardized transparency materials, traceability, or built-in risk management artifacts. If certification no longer requires model-card-like artifacts, HCOs will need to define what documentation they require for predictive decision support (e.g., intended use, limitations, validation population, monitoring plan) as part of procurement and governance.

Downstream implications HCOs may experience

- More integration opportunity, more governance responsibility: If the ecosystem shifts toward API-first interoperability, innovation teams may find it easier to pilot third-party tools, including analytics and AI systems; however, the burden of evaluating safety, appropriateness, documentation quality (including whether you require model cards or equivalent), and monitoring will shift more to hospital governance rather than being implicitly shaped by certification criteria.
- Operational "friction" becomes information blocking-adjacent for automated/AI-enabled uses: Because HTI-5 clarifies that automated/AI-enabled access/use is within the scope of Part 171 concepts, HCOs should expect increased need for consistent internal policies on API enablement, third-party app review, authentication/authorization practices, and documented rationales for limitations or denials.
- Clinical leadership should plan for stronger local standards: Clinical/Quality/Safety leaders should anticipate more internal work to define "acceptable evidence," governance checkpoints, and monitoring requirements for AI/CDS features, particularly as certification becomes less prescriptive in this domain.

7. Analysis

HTI-5 has potential to create overall benefits for HCOs because it emphasizes what scales effectively: modern, standards-based, FHIR-first APIs. Done well, that direction makes interoperability more modular (apps and services can plug in without bespoke interfaces), more scalable (automation and bulk workflows become feasible), and more measurable (uptime, latency, error rates, coverage can be monitored). In that sense, the proposal can accelerate a shift away from document-centric exchange patterns and toward a platform model where patient access, third-party tools, and cross-system workflows are easier to implement and iterate, especially if vendors compete on API performance and developer experience.

The concern is that modern APIs don't make the old safeguards unnecessary; they often make them more important. APIs expand the number of entry points to EHI and increase the number of actors and workflows in the data path (apps, exchanges, automation services), which raises the need for strong access governance, better auditing, and operational playbooks. Many of the removed criteria were less about "legacy exchange" and more about assurance mechanisms: controls, documentation, design/process expectations, and testable evidence. Removing them doesn't eliminate underlying obligations (e.g., HIPAA security expectations), but it does remove a federal test harness that created some uniformity and proof. At the same time, HTI-5's information blocking direction makes automated access/use (including AI-enabled workflows) feel more "mainstream," which can create operational tension: organizations may be pressured to enable access faster and more broadly while having fewer certification-backed artifacts to rely on when managing risk.

Ultimately, the outcome hinges on whether HCOs treat this as a shift from "certification as assurance" to ecosystem assurance driven by buyer governance and governance across vendors, third-party apps, identity/authorization, and exchange partners. To make the rule a net good, HCOs will likely need to:

1. Re-specify non-negotiables (security controls, auditability, accessibility, documentation expectations) through contracting and security review
2. Invest in API observability and scope-aware auditing so "measurable" becomes real
3. Validate safety at the workflow level (patient matching, data freshness, semantic integrity, automation failure modes).

HTI-5 has the potential to be a catalyst for faster interoperability, but only if HCOs deliberately rebuild the assurance layer that certification previously carried by default.

8. What HCOs Should Do Now

0–3 months:

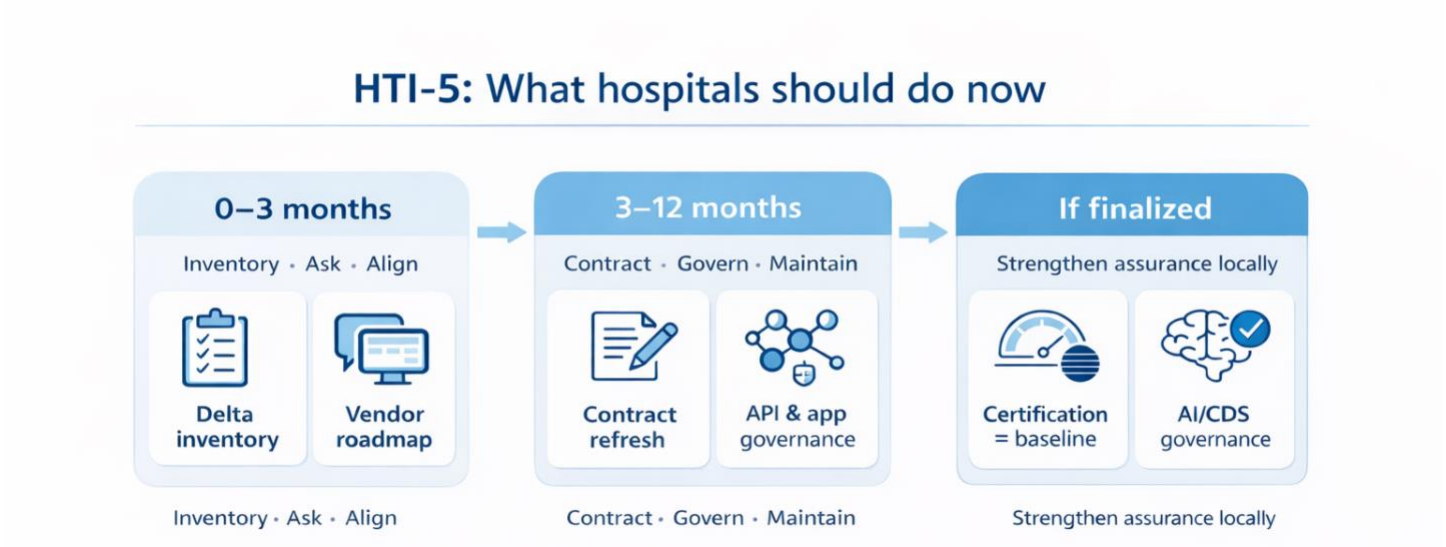
- Build a "HTI-5 delta inventory": a list of capabilities you rely on today that are proposed for removal from certification (privacy/security, public health interfaces, app access functions)
- Ask your EHR vendor:
  - Which removed criteria will they continue to support "as product," vs. "optional module," vs. "deprecate"?
  - What changes are planned for patient access (VDT) and accessibility conformance expectations?
- Align compliance and IT Security: Which controls do you need to retain or establish, regardless of certification scope (e.g., auditing, encryption, access control patterns)?

3–12 months:

- Contract refresh / addenda review: Add explicit language for any removed criteria you still require (audit logging detail, encryption at rest/in transit, authentication controls, etc.).
- API & third-party app governance: Update app onboarding procedures, scope approval, rate limiting governance, and documentation of denials/delays to align with the proposed direction of information blocking modernization.
- Public health & reporting roadmap: Identify which public health reporting interfaces are mission-critical locally, independent of certification status, and plan how you will maintain them if vendor incentives shift.

If finalized as proposed:

1. Treat ONC certification as a narrower baseline and strengthen internal governance, security assurance, and contracting to compensate for removed certification requirements.
2. Stand up (or reinforce) a hospital AI/CDS governance program that requires vendor documentation, model limitations, monitoring, and safety review, especially if certification-side transparency requirements diminish.



9. Questions for HCO Leaders to Ask

HTI-5's direction (i.e., streamlining certification while clarifying that automated access and use of EHI are in scope for information blocking) shifts more of the "assurance burden" to HCOs. The most important leadership questions are therefore not only "What will our vendor do?" but "What will we require, monitor, and govern locally to keep interoperability safe, reliable, and auditable?" The questions below are designed to surface where your organization is relying on certification as a proxy for assurance, where you need stronger contracting and technical controls, and where your operating model for APIs, apps, and decision support needs to mature.

A. Strategy & accountability

1. What is our "interoperability strategy" if certification becomes a narrower floor?
    a. Primary owners to answer: CIO / interoperability lead; procurement; legal
    b. Why this matters: Without assuming certification covers everything, you need an explicit stance on what you will still require (security controls, documentation, accessibility, service levels).
    c. What a good answer looks like: A short policy statement plus a one-page "minimum requirements" list used in procurement and governance.
2. Who owns interoperability risk end-to-end (not just the EHR team)?
    a. Primary owners to answer: CIO; CISO; compliance/privacy; CMIO
    b. Why this matters: API/app risk crosses IT, security, privacy, clinical leadership, operations, and innovation; gaps happen when ownership is ambiguous.
    c. What a good answer looks like: Named accountable executive(s), a RACI, and a standing governance forum for app enablement and data access.
3. What is our posture on third-party app enablement (default allow vs default deny vs tiered)?
    a. Primary owners to answer: Compliance/privacy; security; CMIO; interoperability lead
    b. Why this matters: HTI-5 reinforces that automated access/use is within the policy frame; inconsistent decision-making increases information blocking and security risk.
    c. What a good answer looks like: A tiered policy (low/medium/high risk apps) with clear criteria and predictable timelines for decisions.

B. Vendor roadmap & contracting

1. What changes will our vendors implement, deprecate, or repackage as optional modules?
    a. Primary owners to answer: EHR vendor management; CIO/IT apps; vendor account teams
    b. Why this matters: Even if HCOs aren't directly regulated by Part 170, vendor roadmaps drive hospital costs, timelines, and operational impacts, especially for public health reporting (eCR, AUR, cancer registries), where certification changes may shift support models.
    c. What a good answer looks like: A written vendor "HTI-5 impact statement," including what features remain, what's removed, and what becomes add-on.
2. What assurance will we require contractually if certification no longer mandates it?
    a. Primary owners to answer: Legal; procurement; security; risk/compliance
    b. Why this matters: If audit/security/accessibility/process requirements are removed from certification, HCOs may need to require them by contract and validate them.
    c. What a good answer looks like: Contract clauses requiring minimum controls and evidence artifacts (e.g., audit logs, MFA, encryption, SOC2), plus incident and escalation obligations.
3. Do our contracts cover API performance, reliability, and support obligations?
    a. Primary owners to answer: IT apps/interoperability; vendor management; legal
    b. Why this matters: "FHIR-first" only works if APIs are dependable and measurable; without SLAs, downtime becomes operational risk.
    c. What a good answer looks like: Defined metrics (uptime, latency, error rates), reporting cadence, joint monitoring, and remedies.

C. Information blocking readiness

1. When we restrict or delay access, do we have a consistent, documented rationale and workflow?
    a. Primary owners to answer: Compliance/privacy; legal; HIM; interoperability; security
    b. Why this matters: If automated access/use is in scope, you need repeatable decision pathways and documentation to support legitimate constraints.
    c. What a good answer looks like: SOPs for app denials/restrictions, including documented risk basis, exception logic where applicable, and review cadence.
2. Are our rate limiting and access controls defensible clinically and operationally?
    a. Primary owners to answer: Security; interoperability; IT operations; CMIO
    b. Why this matters: Controls are necessary but can look like "blocking" if arbitrary; you want controls that are consistent and risk-based.
    c. What a good answer looks like: Policies for throttling/scopes tied to availability/security risk, evidence of monitoring, and periodic reassessment.
3. How do we handle patient-authorized third-party access requests at scale?
    a. Primary owners to answer: Patient access/digital front door; HIM; compliance/privacy; interoperability
    b. Why this matters: Increased app ecosystem demand creates operational load and risk; one-off handling doesn't scale.
    c. What a good answer looks like: Standard intake and enablement process, patient-facing guidance, escalation channels, and clear turnaround times.

D. Security, privacy, and auditability in an API-first world

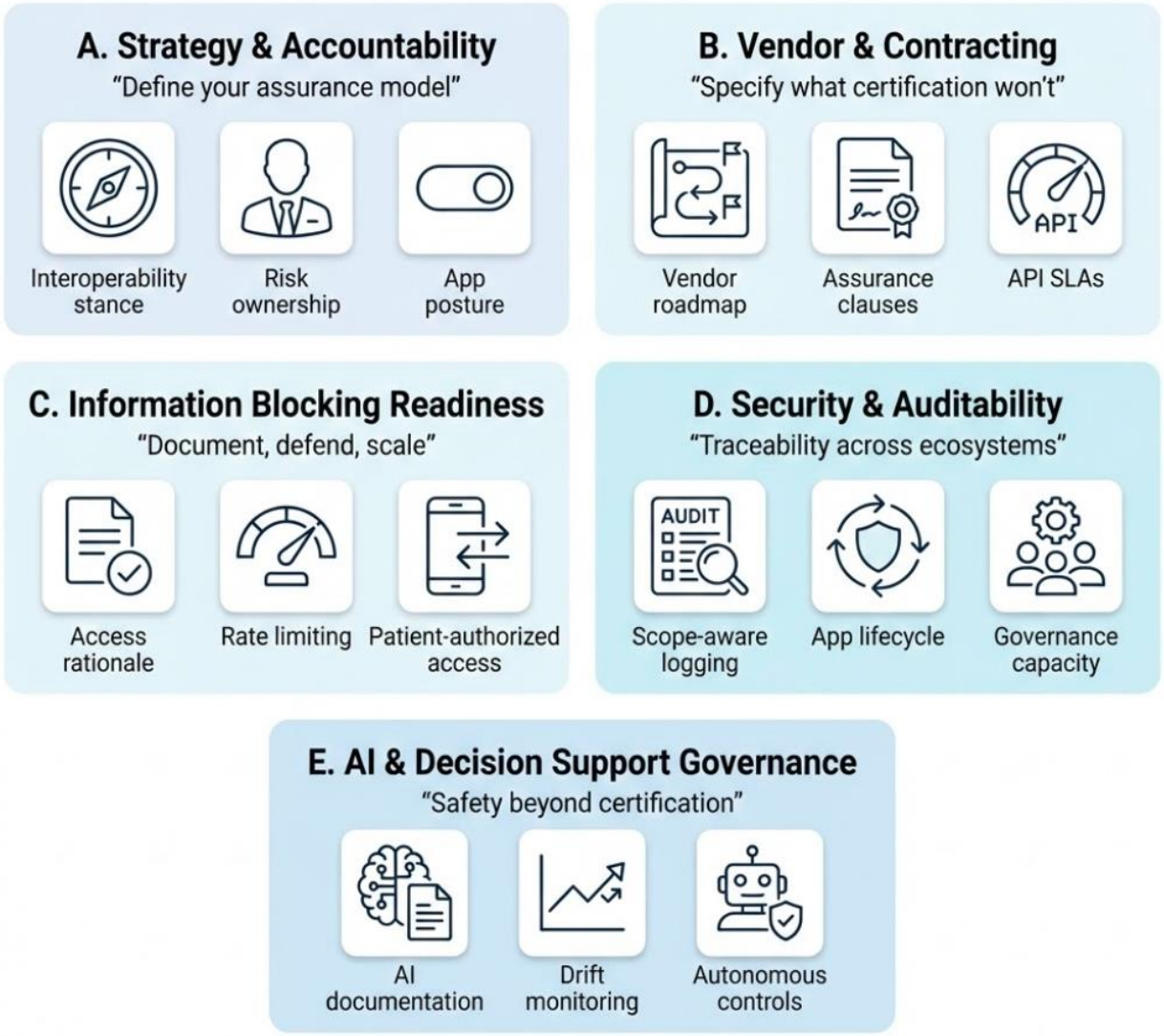
1. Can we answer: "Who accessed what data, for which patient, when, and why?" across apps?
    a. Primary owners to answer: Security; privacy; IT operations; data governance
    b. Why this matters: API ecosystems multiply access points; auditability is the core safety/compliance control in a modular environment.
    c. What a good answer looks like: Scope-aware logging, centralized monitoring, and ability to trace access across EHR + apps + middleware.
2. Do we have an app onboarding/offboarding playbook?
    a. Primary owners to answer: Security; IT operations; compliance; vendor management
    b. Why this matters: The biggest gaps occur at boundaries—approval, credential revocation, and incident response.
    c. What a good answer looks like: A documented playbook with roles, steps, timelines, breach response, and clear authority to suspend access quickly.
3. Are we resourced to govern an expanding app ecosystem?
    a. Primary owners to answer: CIO; CISO; operations leadership; PMO/service management
    b. Why this matters: Policy fails without capacity—security review, privacy assessment, technical validation, and ongoing monitoring.
    c. What a good answer looks like: Dedicated roles, a service model with intake/SLAs, and standard templates/checklists.

E. AI and decision support governance

1. What documentation do we require for predictive decision support (embedded or third-party)?
    a. Primary owners to answer: CMIO; clinical quality/safety; AI governance; procurement; vendor
    b. Why this matters: If certification is less prescriptive, HCOs need to set their own minimum transparency bar.
    c. What a good answer looks like: Required "AI documentation packet" (intended use, limitations, validation population, monitoring plan, escalation).
2. How will we monitor model drift, performance, and safety events over time?
    a. Primary owners to answer: AI governance; quality/safety; analytics; IT ops; vendor

b. Why this matters: Predictive tools can degrade; lack of monitoring turns "innovation" into latent safety risk.
c. What a good answer looks like: Defined metrics, review cadence, alert thresholds, and change-control for model updates.

3. Do we have a governance path for "agentic" workflows that act autonomously?
   a. Primary owners to answer: AI governance; risk/compliance; security; CMIO; legal
   b. Why this matters: Autonomy raises stakes for controls and oversight; "automated use" is explicitly within the policy frame.
   c. What a good answer looks like: Clear policy on what can be autonomous vs human-in-the-loop, required auditability, and escalation pathways.



10. Conclusions

HTI-5 is best viewed as a rebalancing of federal oversight: fewer prescriptive certification requirements, more emphasis on modern interoperability via APIs, and continued attention to information blocking as the lever to promote real-world access, exchange, and use of EHI. For HCOs, this likely means greater variability across vendor implementations and greater responsibility to define minimum expectations for security controls, accessibility, public health reporting, and AI/CDS governance independent of certification. The near-term goal is not to wait for the final rule, but to ensure we can rapidly adapt: specify what we require, document why, and align workflows so that interoperability and app enablement are safe, supportable, and compliant.

References and Resources

- About HTI-5:
  - Press Release (ONC/ASTP)
  - HTI-5 Proposed Rule (ONC/ASTP main page)
  - HTI-5 Proposed Rule Fact Sheet (ONC/ASTP)
  - HTI-5 Proposed Rule full text (Federal Register)

- What HTI-5 Changes:
  - § 170.315 ONC certification criteria for Health IT
  - ONC Health IT Certification Program Test Method

- Other Related Resources:
  - ONC/ASTP Certification Program Overview
  - Certified Health IT Product List
  - United States Core Data for Interoperability (USCDI)
  - Information Blocking (ONC/ASTP)
  - CMS Interoperability Framework
  - CMS Health Technology Ecosystem Initiative

To cite this report:
Espinoza J; Rising T1DE Alliance. *HTI-5 Proposed Rule: What It Means for Healthcare Organizations Using Certified Health IT*. White paper. Published February 10, 2026. https://risingt1dealliance.org/

About the Rising T1DE Alliance

Founded in 2016 at Children's Mercy Hospital (Kansas City), the Rising T1DE Alliance (RTA) was created to proactively identify and address clinical risks in type 1 diabetes through actionable, timely insights. With initial support from The Leona M. and Harry B. Helmsley Charitable Trust, and additional funding in 2020, RTA developed the Diabetes Data Dock (D-Data Dock)—a cloud-based population health management platform that integrates data from the electronic health record (EHR), self-management devices (including CGM), patient-reported outcomes, and other sources.

RTA's work has demonstrated that integrating CGM with clinical/EHR context enables more actionable decision support than CGM-only approaches. While early deployment focused on leading academic sites, RTA has increasingly emphasized that every person with diabetes deserves data-driven care, regardless of where they receive care, including in rural and low-resource settings through hub-and-spoke models. Learn more at www.risingt1dealliance.org.

Mission

The RTA strives to revolutionize type 1 diabetes care through data-driven, patient-centered care.

Vision

We're reimagining diabetes care into a paradigm that continuously and seamlessly integrates data, technology, and personalized care delivery, while enabling rapid learning to optimize health outcomes.

Values

- Patient-Centered Care: People and their lived experiences are at the core of our efforts, ensuring every intervention supports individual needs and well-being.
- Data-Driven Innovation: We push healthcare innovation using analytics and machine learning to transform real-time health data into actionable insights.
- Learning & Adaptability: Rooted in implementation science; we refine and enhance interventions as needs evolve.
- Collaboration & Advocacy: We leverage a diverse network of institutions, patient advocates, and research organizations to drive change.
- Integrity & Transparency: We uphold high ethical standards and transparently share findings and methodologies to encourage adoption.
- Equity & Access: Everyone deserves high-quality diabetes care; we dismantle barriers with scalable solutions for diverse communities.
- Sustainability: We create tools and models that enable economically viable care for patients, health systems, and payers.

RISING T1DE ALLIANCE

Appendix 1: Key Definitions and Acronyms

A. Acronyms (alphabetical)

- ACB: *ONC-Authorized Certification Body.* An entity authorized by ONC to test and certify health IT under the ONC Health IT Certification Program.
- AI: *Artificial intelligence.* In this memo, used broadly (including machine learning) as discussed in HTI-5's "AI-enabled future" framing.
- API: *Application programming interface.* A technical interface that enables software applications to access data/services; HTI-5 emphasizes modern exchange through standards-based APIs.
- ASTP/ONC: *Assistant Secretary for Technology Policy / Office of the National Coordinator for Health Information Technology.* HHS office responsible for the ONC certification program and (with OIG/CMS) information blocking policy.
- AUR: *Antimicrobial Use and Resistance reporting*. A public health reporting capability that enables electronic submission of antimicrobial use and resistance data to public health agencies
- Bulk FHIR®: A FHIR-based approach for bulk data export (population-level). Often referenced as "Bulk FHIR API" in certification context.
- CDS: *Clinical decision support.* Tools that provide clinicians or patients with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care. (The memo uses CDS as a familiar umbrella; rely on the rule text for any binding definitions.)
- CFR: *Code of Federal Regulations.* The codified rules, including 45 CFR Part 170 (certification) and Part 171 (information blocking).
- DSI: *Decision Support Intervention*. A type of clinical decision support functionality referenced in the ONC certification criteria (e.g., "Decision support interventions," § 170.315(b)(11))
- eCR: *Electronic Case Reporting*. A public health reporting capability that enables automated electronic submission of reportable disease cases from certified health IT to public health agencies.
- EHI: *Electronic health information.* The category of information used in the information blocking regulation; central to Part 171.
- EHR: *Electronic health record.* A health IT system commonly certified under ONC's program (or composed of certified modules).
- FHIR®: *Fast Healthcare Interoperability Resources.* A standards framework commonly used for APIs; HTI-5 frames FHIR-based APIs as foundational.
- HCOs: *Healthcare Organizations*
- HHS: U.S. Department of Health and Human Services.
- HTI: *Health Data, Technology, and Interoperability.* The naming convention for ONC rulemakings.
- HTI-5: The HTI-5 Proposed Rule ("Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity").
- ONC Health IT Certification Program: The federal program that certifies health IT against defined criteria (45 CFR Part 170). HTI-5 proposes to streamline/narrow criteria.
- QMS: *Quality management system.* A set of policies/processes for design, development, quality assurance; referenced as a certification criterion in baseline regimes and proposed for removal.
- TEFCA: *Trusted Exchange Framework and Common Agreement.* A national framework for health information exchange; HTI-5 includes related discussion and policy context (details vary by rule section).
- USCDI: *United States Core Data for Interoperability.* A standardized dataset used in certification and interoperability policy.
- VDT: *View, Download, and Transmit.* The patient access capability in certified health IT (§ 170.315(e)(1)) that enables individuals to view, download, and transmit their electronic health information to third parties.

B. Important definitions

- Certification criterion (Part 170): A specific functional or technical capability that a health IT product must demonstrate to be certified under the ONC program. HTI-5 proposes eliminating many criteria and revising others.
- Certified health IT/certified module: Health IT that has been certified to one or more ONC certification criteria by an ONC-ACB. HCOs often use a certified EHR and/or additional certified modules.
- Information blocking (Part 171): A regulated concept describing practices that are likely to interfere with the access, exchange, or use of EHI, subject to defined exceptions. HTI-5 proposes updates intended to better promote EHI access/exchange/use.
- Access / exchange / use (EHI): Core concepts in information blocking policy. HTI-5's framing emphasizes that EHI should be available for access/exchange/use, including through innovative software.
- Actor *(information blocking context)*: The categories of persons/entities subject to Part 171 (e.g., health care providers, health IT developers of certified health IT, and health information networks/exchanges). (When you finalize, cite the precise definitional section from the proposed rule text.)
- Exception *(information blocking context)*: A defined "safe harbor" category of practices that are not treated as information blocking if all conditions of the exception are met (e.g., certain privacy/security-related limits). HTI-5 proposes revisions intended to address misuse and improve enforceability.

C. Practical translation guide

- "Certification criteria" = what ONC requires *vendors* to show for certification; HTI-5 proposes removing many of these.
- "Information blocking" = rules that can apply to *how providers and vendors behave* when others seek access/exchange/use of EHI; HTI-5 proposes updates meant to make access/exchange/use more consistent.
- "FHIR / APIs" = the direction of travel for interoperability; HTI-5 frames these as foundational, including for an AI-enabled future.

Appendix 2: Status of the Current Certification Criteria Under HTI-5

Reference	Certification Criterion	Proposed Action	Timing
§ 170.213	United States Core Data for Interoperability (USCDI)	RETAINED	-
§ 170.315(a)(1)	Computerized provider order entry (CPOE) – medications	RETAINED	-
§ 170.315(a)(2)	Computerized provider order entry (CPOE) – laboratory	RETAINED	-
§ 170.315(a)(3)	Computerized provider order entry (CPOE) – diagnostic imaging	RETAINED	-
§ 170.315(a)(4)	Drug-drug, drug-allergy interaction checks for CPOE	RETAINED	-
§ 170.315(a)(5)	Patient demographics and observations	REVISE	Effective date of final rule
§ 170.315(a)(12)	Family health history	REMOVE	Effective January 1, 2027
§ 170.315(a)(14)	Implantable device list	REMOVE	Effective date of final rule
§ 170.315(a)(15)	Social, psychological, and behavioral data	RETAINED	-
§ 170.315(b)(1)	Transitions of care	REVISE	Effective January 1, 2027
§ 170.315(b)(2)	Clinical information reconciliation and incorporation	REMOVE	Effective January 1, 2027
§ 170.315(b)(3)	Electronic prescribing	RETAINED	-
§ 170.315(b)(6)	Data export	RETAINED	-
§ 170.315(b)(7)	Data segmentation for privacy – send	REMOVE	Effective date of final rule
§ 170.315(b)(8)	Data segmentation for privacy – receive	REMOVE	Effective date of final rule
§ 170.315(b)(9)	Care plan	REMOVE	Effective date of final rule
§ 170.315(b)(10)	Electronic health information export	RETAINED	-
§ 170.315(b)(11)	Decision support interventions	REVISE	Effective date of final rule
§ 170.315(c)(1)	Record and export	RETAINED	-
§ 170.315(c)(2)	Import and display	RETAINED	-
§ 170.315(c)(3)	Clinical quality measures (CQMs) — report	REVISE	Effective date of final rule
§ 170.315(c)(4)	Clinical quality measures (CQMs) — filter	REMOVE	Effective January 1, 2027
§ 170.315(d)(1)	Authentication, access control, and authorization	REMOVE	Effective date of final rule
§ 170.315(d)(2)	Auditable events and tamper-resistance	REMOVE	Effective date of final rule
§ 170.315(d)(3)	Audit report(s)	REMOVE	Effective date of final rule
§ 170.315(d)(4)	Amendments	REMOVE	Effective date of final rule
§ 170.315(d)(5)	Automatic access time-out	REMOVE	Effective date of final rule
§ 170.315(d)(6)	Emergency access	REMOVE	Effective date of final rule
§ 170.315(d)(7)	End-user device encryption	REMOVE	Effective date of final rule
§ 170.315(d)(8)	Integrity	REMOVE	Effective date of final rule
§ 170.315(d)(9)	Trusted connection	REMOVE	Effective date of final rule
§ 170.315(d)(10)	Auditing actions on health information	REMOVE	Effective date of final rule
§ 170.315(d)(11)	Accounting of disclosures	REMOVE	Effective date of final rule
§ 170.315(d)(12)	Encrypt authentication credentials	REMOVE	Effective date of final rule
§ 170.315(d)(13)	Multi-factor authentication	REMOVE	Effective date of final rule
§ 170.315(e)(1)	View, download, and transmit to 3rd party	REVISE	Effective date of final rule
§ 170.315(e)(2)	Secure messaging	RETAINED	-
§ 170.315(e)(3)	Patient health information capture	REMOVE	Effective January 1, 2027

§ 170.315(f)(1)	Transmission to immunization registries	RETAINED	-
§ 170.315(f)(2)	Transmission to syndromic surveillance	RETAINED	-
§ 170.315(f)(3)	Transmission to electronic reportable lab results	RETAINED	-
§ 170.315(f)(4)	Transmission to cancer registries	REMOVE	Effective January 1, 2027
§ 170.315(f)(5)	Transmission to public health agencies – electronic case reporting	REVISE	Effective date of final rule
§ 170.315(f)(6)	Transmission to public health agencies – antimicrobial use and resistance reporting	REVISE	Effective date of final rule
§ 170.315(f)(7)	Transmission to public health agencies – health care surveys	REMOVE	Effective January 1, 2027
§ 170.315(g)(1)	Automated numerator recording	REMOVE	Effective January 1, 2027
§ 170.315(g)(2)	Automated measure calculation	REMOVE	Effective January 1, 2027
§ 170.315(g)(3)	Safety-enhanced design	REMOVE	Effective date of final rule
§ 170.315(g)(4)	Quality management system	REMOVE	Effective date of final rule
§ 170.315(g)(5)	Accessibility-centered design	REMOVE	Effective date of final rule
§ 170.315(g)(6)	Consolidated CDA creation performance	REMOVE	Effective date of final rule
§ 170.315(g)(7)	Application access — patient selection	REMOVE	Effective January 1, 2027
§ 170.315(g)(8)	Application access — data category request	RETAINED	-
§ 170.315(g)(9)	Application access — all data request	REMOVE	Effective January 1, 2027
§ 170.315(g)(10)	Standardized API for patient and population services	RETAINED	-
§ 170.315(h)(1)	Direct Project	REMOVE	Effective date of final rule
§ 170.315(h)(2)	Direct Project, Edge Protocol, and XDR/XDM	REMOVE	Effective date of final rule
§ 170.315(i)(1)	Automated medication history	RETAINED	-
§ 170.315(j)(11)	Constraint to display (Must Support)	RETAINED	-
§ 170.315(j)(20)	Workflow triggers for decision support interventions	RETAINED	-

Note: The ONC HTI-5 Proposed Rule Chart includes § 170.315(a)(9) "Clinical decision support" (*Remove; effective date of final rule*), but that criterion does not appear in the 60-criterion ONC Health IT Certification Program Test Method; accordingly, § 170.315(a)(9) is not included in the table above.

Summary of Revisions:

- § 170.315(a)(5) Patient demographics and observations: Updates required demographic/ observation data elements and constraints to align with revised interoperability standards and ONC's modernized baseline.
- § 170.315(b)(1) Transitions of care: Revises summary-of-care exchange requirements and timelines, updating what must be supported for sending/receiving standardized transition documentation.
- § 170.315(b)(11) Decision support interventions: Narrows the DSI framework for predictive interventions, removing AI "model card" requirements and scaling back certain transparency/risk-management elements.
- § 170.315(c)(3) Clinical quality measures — report: Revises CQM reporting expectations, updating specifications for how certified health IT must generate and report measures.
- § 170.315(e)(1) View, download, and transmit to 3rd party: Revises patient access/export functionality requirements, aligning expectations for patient-directed transmission and modern API-enabled access pathways.
- § 170.315(f)(5) Electronic case reporting: Updates electronic case reporting requirements and specifications, revising what certified systems must support for public health reporting workflows.
- § 170.315(f)(6) Antimicrobial use and resistance reporting: Updates AUR reporting requirements and specifications, revising what certified systems must support for antimicrobial use/resistance submissions.

Appendix 3: TEFCA in HTI-5

HTI-5's Trusted Exchange Framework and Common Agreement (TEFCA)-related content is narrow and primarily lives in the information blocking portion of the rule (45 CFR Part 171). In short, the proposed rule would remove TEFCA's special "manner" carve-out from the information blocking framework and eliminate the TEFCA-specific subpart that exists solely to support that carve-out.

- What the proposed rule does:
  - Proposes removing the TEFCA Manner Exception (§ 171.403).
  - Because § 171.403 is the only TEFCA-specific exception, proposes removing Part 171 Subpart D (including remaining TEFCA-related sections that would be unnecessary without § 171.403).
- What it means simply:
  - If finalized, organizations generally will not be able to rely on a TEFCA-specific "safe harbor" to say "we will only fulfill this request via TEFCA." Instead, responses would fall under the general information blocking exceptions (e.g., the general Manner Exception, Infeasibility, Privacy/Security exceptions), evaluated case-by-case.
- What it does not do:
  - HTI-5 states that removing § 171.403 does not change obligations under TEFCA itself for entities that are QHINs, Participants, or Sub-participants; it changes only how TEFCA interacts with the information blocking exception structure.
  - HTI-5 also notes that removal of the exception does not automatically make practices that would have fit § 171.403 "information blocking"—they remain subject to the broader "interference" standard and other exceptions.
- Practical implications for HCOs
  - HCOs pursuing TEFCA participation should view this as a policy signal: TEFCA is intended to grow based on adoption and utility, not via a TEFCA-only carve-out in information blocking.
  - Operationally, it reinforces the need for a clear internal approach to "which exchange pathway is appropriate when" (TEFCA vs. other interoperable means such as APIs), grounded in feasibility, security, and patient/partner needs—not blanket "TEFCA-only" policy.

About TEFCA

TEFCA is a national "network-of-networks" framework designed to enable secure, standardized exchange of electronic health information across different health information networks so data can move beyond proprietary boundaries for treatment, patient access, public health, and other permitted purposes. TEFCA is led by ASTP/ONC, and day-to-day operation of the Common Agreement is managed by the Recognized Coordinating Entity (RCE)—currently The Sequoia Project. TEFCA was formally announced in 2022 and became operational in December 2023 when the first Qualified Health Information Networks (QHINs) were designated and data began flowing among them.