Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity (HTI-5) Proposed Rule

February 2026

Disclaimers

- The materials contained in this presentation are based on the proposals in the "Health Data, Technology, and Interoperability: ASTP/ONC Deregulatory Actions to Unleash Prosperity" (HTI-5) Proposed Rule. While every effort has been made to ensure the accuracy of this restatement of those proposals, this presentation is not a legal document. The official proposals are contained in the proposed rule.

- ASTP/ONC must protect the rulemaking process and comply with the Administrative Procedure Act. During the rulemaking process, ASTP/ONC can only present the information that is in the proposed rule as it is contained in the proposed rule. ASTP/ONC cannot interpret that information, nor clarify or provide any further guidance.

- Comments must be submitted through the formal comment submission process as specified in the Federal Register to receive full consideration.

- This communication is produced and disseminated at U.S. taxpayer expense.

AGENDA

- Overview

- ONC Health IT Certification Program
    - ONC Certification Criteria for Health IT
    - Standards and Implementation Specifications for Health Information Technology
    - Terms and Definitions
    - Condition and Maintenance of Certification Requirements
    - ONC Health IT Certification Program Administrative Requirements

- Information Blocking

HTI-5 Proposed Rule

URL: HealthIT.gov/Proposedrule

Purpose of the HTI-5 Proposed Rule

Implementing the 21st Century Cures Act

- Application Programming Interfaces (APIs) that allow electronic health information (EHI) from such technology to be accessed, exchanged, and used without special effort through the use of APIs or successor technology or standards

- Reasonable and necessary activities that do not constitute information blocking

Achieving the Goals of the Trump Administration Executive Orders

- Executive Order (EO) 14192 "Unleashing Prosperity Through Deregulation"

- EO 14267 "Reducing Anti-Competitive Regulatory Barriers"

- EO 14179 "Removing Barriers to American Leadership in Artificial Intelligence"

Leveraging Health IT and Advancing Interoperability

- HITECH Act

- Interoperability Advancement – transition to Fast Healthcare Interoperability Resources (FHIR®) – based APIs

- ONC Health IT Certification Program

Reduce
Outdated and redundant certification requirements

Reset
The regulatory foundation for future FHIR-based interoperability

Refine
The ONC Health IT Certification Program and the Information Blocking Regulations

Improve electronic health information access, exchange, and use

Goals of the HTI-5 Proposed Rule

The HTI-5 Proposed Rule has three core goals:

1. Reducing burden on health IT developers by streamlining the ONC Health IT Certification Program (Certification Program) by removing redundant requirements;

2. Updating the information blocking regulations to better promote EHI access, exchange, and use so that patients' access to their data is not blocked; and

3. Advancing a new foundation of Fast Healthcare Interoperability Resources (FHIR®)-based application programming interfaces (APIs) that promote AI-enabled interoperability solutions through modernized standards and certification.

Cost Savings:

- $1.53 billion, including $650 million over the next 5 years for health IT developers, providers, and other stakeholders.

- The proposed revisions and removal of certification criteria from the Certification Program are estimated to save certified health IT developers more than 1.4 million compliance hours in their first year (an average savings of 4,000 hours per developer) – giving developers new capacity to deliver innovative solutions for their customers.

- The proposed deregulatory actions reduce the effort of developers of certified health IT to meet ongoing Certification Program requirements and reduce barriers to entry for new Certification Program participants.

ONC Health IT Certification Program

ASTP   Better health enabled by data

HHS

HTI-5 Proposed Rule | Proposed Removals or Revisions of Certification Criteria

Certification Criteria	Reference	Remove/Revise	Timing
Patient demographics and observations	§ 170.315(a)(5)	Revise	Effective date of final rule
Clinical decision support	§ 170.315(a)(9)	Remove	Effective date of final rule
Family health history	§ 170.315(a)(12)	Remove	Effective January 1, 2027
Implantable device list	§ 170.315(a)(14)	Remove	Effective date of final rule
Transitions of care	§ 170.315(b)(1)	Revise	Effective January 1, 2027
Clinical information reconciliation and incorporation	§ 170.315(b)(2)	Remove	Effective January 1, 2027
Security tags - summary of care - send	§ 170.315(b)(7)	Remove	Effective date of final rule
Security tags - summary of care - receive	§ 170.315(b)(8)	Remove	Effective date of final rule
Care plan	§ 170.315(b)(9)	Remove	Effective date of final rule
Decision support interventions	§ 170.315(b)(11)	Revise	Effective date of final rule
Clinical quality measures — report	§ 170.315(c)(3)	Revise	Effective date of final rule
Clinical quality measures — filter	§ 170.315(c)(4)	Remove	Effective January 1, 2027
Authentication, access control, authorization	§ 170.315(d)(1)	Remove	Effective date of final rule
Auditable events and tamper-resistance	§ 170.315(d)(2)	Remove	Effective date of final rule
Audit report(s)	§ 170.315(d)(3)	Remove	Effective date of final rule
Amendments	§ 170.315(d)(4)	Remove	Effective date of final rule
Automatic access time-out	§ 170.315(d)(5)	Remove	Effective date of final rule
Emergency access	§ 170.315(d)(6)	Remove	Effective date of final rule
End-user device encryption	§ 170.315(d)(7)	Remove	Effective date of final rule
Integrity	§ 170.315(d)(8)	Remove	Effective date of final rule
Trusted connection	§ 170.315(d)(9)	Remove	Effective date of final rule

Certification Criteria	Reference	Remove/Revise	Timing
Auditing actions on health information	§ 170.315(d)(10)	Remove	Effective date of final rule
Accounting of disclosures	§ 170.315(d)(11)	Remove	Effective date of final rule
Encrypt authentication credentials	§ 170.315(d)(12)	Remove	Effective date of final rule
Multi-factor authentication	§ 170.315(d)(13)	Remove	Effective date of final rule
View, download, and transmit to 3rd party	§ 170.315(e)(1)	Revise	Effective date of final rule
Patient health information capture	§ 170.315(e)(3)	Remove	Effective January 1, 2027
Transmission to cancer registries	§ 170.315(f)(4)	Remove	Effective January 1, 2027
Transmission to public health agencies — electronic case reporting	§ 170.315(f)(5)	Revise	Effective date of final rule
Transmission to public health agencies — antimicrobial use and resistance reporting	§ 170.315(f)(6)	Revise	Effective date of final rule
Transmission to public health agencies — health care surveys	§ 170.315(f)(7)	Remove	Effective January 1, 2027
Automated numerator recording	§ 170.315(g)(1)	Remove	Effective January 1, 2027
Automated measure calculation	§ 170.315(g)(2)	Remove	Effective January 1, 2027
Safety-enhanced design	§ 170.315(g)(3)	Remove	Effective date of final rule
Quality management system	§ 170.315(g)(4)	Remove	Effective date of final rule
Accessibility-centered design	§ 170.315(g)(5)	Remove	Effective date of final rule
Consolidated CDA creation performance	§ 170.315(g)(6)	Remove	Effective date of final rule
Application access — patient selection	§ 170.315(g)(7)	Remove	Effective January 1, 2027
Application access — all data request	§ 170.315(g)(9)	Remove	Effective January 1, 2027
Direct Project	§ 170.315(h)(1)	Remove	Effective date of final rule
Direct Project, Edge Protocol, and XDR/XDM	§ 170.315(h)(2)	Remove	Effective date of final rule

Certification Program Requirements *

Mandatory Certification Criteria

Quality Management System - (g)(4)	Accessibility-Centered Design - (g)(5)

Conditional Certification Criteria

Authentication, Access Control, Authorization - (d)(1)	Integrity - (d)(8)
Auditable Events and Tamper-Resistance - (d)(2)	Trusted Connection - (d)(9)
Audit Report(s) - (d)(3)	Auditing Actions on Health Information - (d)(10)
Amendments - (d)(4)	Encrypt Authentication Credentials – (d)(12)
Automatic Access Time-Out - (d)(5)	Multi-factor Authentication - (d)(13)
Emergency Access - (d)(6)	Safety Enhanced Design - (g)(3)
End-User Device Encryption - (d)(7)	Consolidated CDA Creation Performance - (g)(6)

Certification Criteria *Not* Associated with Medicare Promoting Interoperability Program and the Promoting Interoperability performance category under the Merit-based Incentive Payment System

Social, Psychological, and Behavioral Data - (a)(15)	
Security Tags – Summary of Care – Send - (b)(7)	Care Plan - (b)(9)
Security Tags – Summary of Care – Receive - (b)(8)	Accounting of Disclosures - (d)(11)

Key:
Red = Removal (effective date of a Final Rule);
Grey = No changes

* These columns identify mandatory and conditional certification requirements (i.e., the application of certain certification criteria to Health IT Modules) that Health IT Modules presented for certification must meet regardless of the setting or program the Health IT Module is designed to support.

Certification Criteria
Associated with Medicare Promoting Interoperability Program and the Promoting Interoperability performance category under the Merit-based Incentive Payment System[+]

Implantable Device List - (a)(14)	Patient Demographics and Observations - (a)(5)	Workflow Triggers for Decision Support Interventions – Clients – (j)(20)
Direct Project - (h)(1)	Transitions of Care - (b)(1)	Subscriptions – Client – (j)(21)
Direct Project, Edge Protocol, and XDR/XDM - (h)(2)	Decision Support Interventions - (b)(11)	CPOE – Medications - (a)(1)
Family Health History - (a)(12)	View, Download, and Transmit to 3rd Party - (e)(1)	CPOE – Laboratory - (a)(2)
Clinical Information Reconciliation and Incorporation - (b)(2)	Transmission to PHAs – Electronic Case Reporting - (f)(5) - shifting to functional	CPOE – Diagnostic Imaging - (a)(3)
CQM Filter – (c)(4) *optional	Transmission to PHAs – Antimicrobial Use and Resistance Reporting - (f)(6) - functional	Drug-Drug, Drug-Allergy Interaction Checks for CPOE - (a)(4)
		Electronic Health Information Export - (b)(10)
Patient Health Information Capture - (e)(3)	CQM – Report - (c)(3)	CQM – Record and Export - (c)(1)
Transmission to Cancer Registries - (f)(4) (retire standard along with criterion)	Electronic Prescribing - (b)(3)	CQM – Import and Calculate - (c)(2)
Transmission to PHAs – Health Care Surveys - (f)(7)	Real Time Prescription Benefit – (b)(4)	Transmission to Immunization Registries - (f)(1)
Automated Numerator Recording - (g)(1)	Provider Prior Authorization API – Coverage Requirements Discovery – (g)(31)	Transmission to PHAs – Syndromic Surveillance - (f)(2)
Automated Measure Calculation – (g)(2)	Provider Prior Authorization API – Documentation Templates and Rules – (g)(32)	Transmission to PHAs – Reportable Laboratory Tests and Values/Results - (f)(3)
Application Access – Patient Selection - (g)(7)		
Application Access – All Data Request - (g)(9)	Provider Prior Authorization API – Prior Authorization Support - (g)(33)	Standardized API for Patient and Population Services – (g)(10)

Key:
Red = Removal (effective date of a Final Rule); Light Red = Removal with transition (Jan 1, 2027);
Light Yellow = Revised; Grey = No changes
Blue Font = Base EHR Definition / CEHRT Definition
Green Font = CEHRT Definition only

[+] These programs require the use of Certified EHR Technology (CEHRT) as defined at 42 CFR 414.1305 (eligible clinicians) and 495.4 (eligible hospitals and CAHs).

Privacy and Security Certification Criteria

Future State:

We intend to prioritize the adoption of privacy and security capabilities that are fit for purpose, use case specific, and deliver much needed technical consistency in the market when paired with specific conformance requirements.

- For example, as we pursue more API-focused certification criteria, if the standards and implementation guides adopted for them do not specify or leave optional specific security requirements, we may look to add further constraints (e.g., multi-factor authentication support).

- But in all cases, we intend to make security capability conformance a built-in part of a certification criterion's conformance and not the separate and stand-alone conformance assessment that it is today.

Deregulatory Proposed Rule:

Despite the Certification Program providing various certification flexibilities and approaches to accommodate the privacy and security certification criteria (i.e., different approaches for the 2011, 2014 and 2015 Editions), the costs, burden, and unintended consequences of these requirements far exceed their intended purpose and benefits.

- **Proposal:**
  Remove all the privacy and security certification criteria in § 170.315(d) and the associated Privacy and Security Certification Framework under § 170.550(h) as of the effective date of a subsequent final rule.

- **Alternative Proposal:**
  Retain certain certification criteria related to audits that may serve to help identify fraud and abuse.

Standards and Implementation Specifications for Health Information Technology

- In instances where we propose to remove or revise a certain certification criterion, we also propose to remove the standards that are referenced by the certification criterion.

- In some cases, we propose to remove a standard consistent with a certification criterion transition period (<u>until January 1, 2027</u>).

- In very limited circumstances, we propose to retain a standard referenced by a certification criterion proposed for removal. We do this to support interoperability advancement under the HHS Health IT Alignment Program.
  - For example, we do not propose to remove the Direct Project transport standard in § 170.202(a)(2). The Direct Project standards are widely utilized in various use cases and maintaining the standard will support interoperability.

- We propose to remove standards from the Code of Federal Regulations (CFR) that are outdated and no longer referenced in the Certification Program.

Terms and Definitions - § 170.102

- Revise the "Base EHR" definition

  ‣ Remove references to certification criteria that we have proposed to remove from the CFR

- Remove "Common Clinical Data Set," "Global Unique Device Identification Database (GUDID)," and "Production Identifier"

  ‣ These terms are no longer referenced in 45 CFR part 170

Conditions and Maintenance of Certification Requirements for Health IT Developers

Conforming Edits

We propose to **make conforming edits** for several Conditions and Maintenance of Certification requirements, including:

- *Assurances*

- *Application Programming Interfaces*

- *Attestations*
  - ‣ For example, a health IT developer must provide the Secretary an attestation of compliance with § 170.404, the API Conditions and Maintenance of Certification requirements, according to § 170.406(a)(4). Because we propose to remove § 170.315(g)(7) through (9), we also propose to remove the reference to § 170.315(g)(7) through (9) in § 170.406(a)(4).

Remove and Descope

Real World Testing

We propose to remove requirements and descope "Real World Testing" Condition and Maintenance of Certification requirements with the following deregulatory actions:

- Removing the requirement to submit real world testing plans for all real world testing certification criteria (§ 170.405(b)(1));

- Limiting full real world testing results reporting (§ 170.405(b)(2)) to only Health IT Modules that are certified to the API certification criteria; and

- Permitting the use of the Standards Version Advancement Process (SVAP) for the remaining non-API real world testing certification criteria with minimal reporting requirements.

Insights

We propose to remove and descope measures associated with the "Insights" Condition and Maintenance of Certification requirements to limit reporting requirements only to the "use of FHIR in apps through certified health IT" measure.

ONC Health IT Certification Program Administrative Requirements

We propose to make conforming edits, in subpart E of 45 CFR part 170 (ONC Health IT Certification Program), to remove references to certification criteria that we propose to remove in the proposed rule.

Specifically, in:

- § 170.523

- § 170.550

- § 170.555, and

- § 170.570

As an example, we propose to make conforming revisions to the Principles of Proper Conduct for ONC-ACBs in § 170.523 by removing cross-references to certain certification criteria that we propose to remove. More specifically, we propose to remove and reserve § 170.523(f)(1)(ix) through (xi) which reference the "privacy and security" certification criteria (§ 170.315(d)), the "quality management system" certification criterion (§ 170.315(g)(4)), and the "accessibility-centered design" certification criterion (§ 170.315(g)(5)).

Information Blocking

ASTP   Better health enabled by data

HHS

Current Definitions - § 171.102

Proposal:

Revise the "access" and "use" definitions in § 171.102 to emphasize that the definitions include automated means of access, exchange, or use of EHI — including, without limitation, autonomous AI systems.

Additional "Alternative" Proposal:

In addition to updating the "access" and "use" definitions, potentially similarly revise the "exchange" definition.

Infeasibility Exception - § 171.204

Third party seeking modification use condition - § 171.204(a)(3)

Proposal: Remove.

Manner exception exhausted condition - § 171.204(a)(4)

Proposal: Revise to:

- Require all three "alternative" manners from the Manner Exception alternative manner condition be offered

- Replace "[t]he actor does not provide the same access, exchange, or use of the requested electronic health information to a substantial number of individuals or entities that are similarly situated to the requestor"

  with

  "[t]he actor does not provide analogous access, exchange, or use of the requested electronic health information to any other individual or entity"

  ‣ Essentially, we are proposing to replace "same" with "analogous" and remove the "substantial number" and "similarly situated" conditions.

Alternative Proposal: Remove the condition.

Manner Exception - § 171.301
Manner requested condition - § 171.301(a)

Proposal:

Add text explicitly stating that **any contract or agreement** under which the actor and requestor agree to fulfill a request for access, exchange, or use of EHI, and any license from the actor of interoperability elements used in fulfilling the request in the manner requested:

- Must be at market rate;

- Must not be a contract of adhesion; or

- Must not contain unconscionable terms.

Add definitions to § 171.102 for market rate, contract of adhesion, and unconscionable terms

Alternative Proposal:

- Remove paragraph (a)(2) from the *manner requested* condition of the Manner Exception (excludes application of the Fees and Licensing Exceptions to agreements under paragraph (a) to fulfill requests for EHI in any manner requested.

- Apply the conditions of both the Fees Exception and Licensing Exception to any agreement an actor makes with a requestor related to fulfilling the request for access, exchange, or use of EHI in any manner requested.

Whether or Not a Proposal is Adopted

- The *manner requested* condition only covers the technical manner of exchange of the requested EHI.
- Contracts or agreements for access, exchange, and use of EHI cannot be contracts of adhesion or contracts containing unconscionable terms. These types of contracts are not covered by the Manner Exception even if these agreements were styled as, or in fact were, achieving access, exchange, or use of the requested EHI in the requested manner. These types of contracts would also likely constitute an interference under the information blocking regulations. (90 FR 61012)

Trusted Exchange Framework and Common Agreement (TEFCA) Manner Exception - § 171.403

Proposal:

 Remove the TEFCA Manner Exception (§ 171.403) and associated definitions.

COMMENT PERIOD

📅 Dec. 29, 2025 – Feb. 27, 2026.

🔍 URL: HealthIT.gov/Proposedrule

Resources Available on HealthIT.gov!

Visit https://healthIT.gov/Proposedrule for more information.

→ HTI-5 Press release

→ HTI-5 Proposed Rule Fact Sheet

→ HTI-5 Proposed Rule Information Session Recording

→ Proposed rule at the Federal Register

Reach out via phone or web

📱 202-690-7151

💬 Feedback Form: https://www.healthit.gov/form/healthit-feedback-form

Stay connected, follow us on socials

𝕏 @HHS_TechPolicy

in Assistant Secretary for Technology Policy

▶ Youtube.com/@HHS_TechPolicy

Subscribe to our weekly eblast at healthit.gov for the latest updates!