Office of the National Coordinator for Health Information Technology

ONC Health IT Certification Program Developer Roundtable

March 27, 2024

Disclaimers

- The materials contained in this presentation are based on the provisions contained in 45 C.F.R. Parts 170 and 171. While every effort has been made to ensure the accuracy of this restatement of those provisions, this presentation is not a legal document. The official program requirements are contained in the relevant laws and regulations. Please note that other Federal, state and local laws may also apply.

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

Agenda

1. Opening Remarks
2. HTI-1 Final Rule Overview
3. Test Procedure and CCG Layout Updates

Today's Speakers

1. Robert Anthony, Director, Certification and Testing Division
2. Ashley Hain, Branch Chief, Tools and Testing
3. Jeff Smith, Deputy Director, Certification and Testing Division
4. Jim Younkin, Audacious Inquiry

Office of the National Coordinator for Health Information Technology

HTI-1 Final Rule Overview

Jeff Smith

Discontinuing Year-Themed “Editions”

HTI-1 Final Rule

Discontinues the year-themed editions and establishes a single set of certification criteria, “ONC Certification Criteria for Health IT”

Benefits

- Allows the Certification Program and health IT developers to more effectively utilize new and updated standards and functionality in a timely manner
- Allows users of health IT to work in partnership with health IT developers to update their systems for new standards or functionality in the manner that works best for their unique needs
- Assists health care industry participants in other HHS programs that reference Certification Program standards and criteria, such as CMS’s Promoting Interoperability Program, by ensuring developers provide timely updates for any new or updated certification criteria
- Supports users of health IT by reducing potential confusion of tracking use of different editions of certified health IT

Establishing Applicability and Expiration Dates for Certification Criteria and Standards

HTI-1 Final Rule

- Establishes the dates by which a prior version of a criterion is no longer applicable when a revised version (including new and revised standards) of that criterion is adopted
- Establishes applicable timelines, including expiration dates, for the adoption of standards when a new, revised, or updated version of the standard is adopted for the same purpose

Benefits

- Supports establishment of clear timelines associated with the specific criterion or standard

- Facilitates ease of reference for federal, state, local or tribal programs seeking to align their program requirements to the standards and implementation specifications available in certified health IT
- Ensures that customers are provided with timely technology updates

United States Core Data for Interoperability (USCDI) v3

- Adopted USCDI v3 as the new baseline for certification.
- Expanding the data elements and data classes included in USCDI increases the amount of data available to be used and exchanged for patient care.
    - ONC is expanding the USCDI by moving from USCDI v1 to the adoption of USCDI v3 in 45 CFR 170.213(b) by **January 1, 2026**. Until that time, both versions will be accepted as in compliance with the USCDI standard in § 170.213.
- Health IT Modules certified to criteria that reference USCDI would need to update to USCDI v3 by the January 1, 2026, using the applicable US Core IG and C-CDA Companion Guide:

- § 170.315(b)(1): Transitions of Care
- § 170.315(b)(2): Clinical Information Reconciliation and Incorporation
- § 170.315(b)(9): Care Plan*
- § 170.315(e)(1): View, Download, and Transmit 3rd Party
- § 170.315(g)(6): Consolidated CDA Creation Performance
- § 170.315(g)(9): Application Access-All Data Request
- § 170.315(g)(10): Standardized API for Patient and Population Service

* § 170.315(b)(9) is only updated to the C-CDA Companion Guide

USCDI v3

New Data Classes and Elements Data Element Reclassified Name and Other Changes to Existing Data Classes/Elements

Patient Requested Restrictions

Background

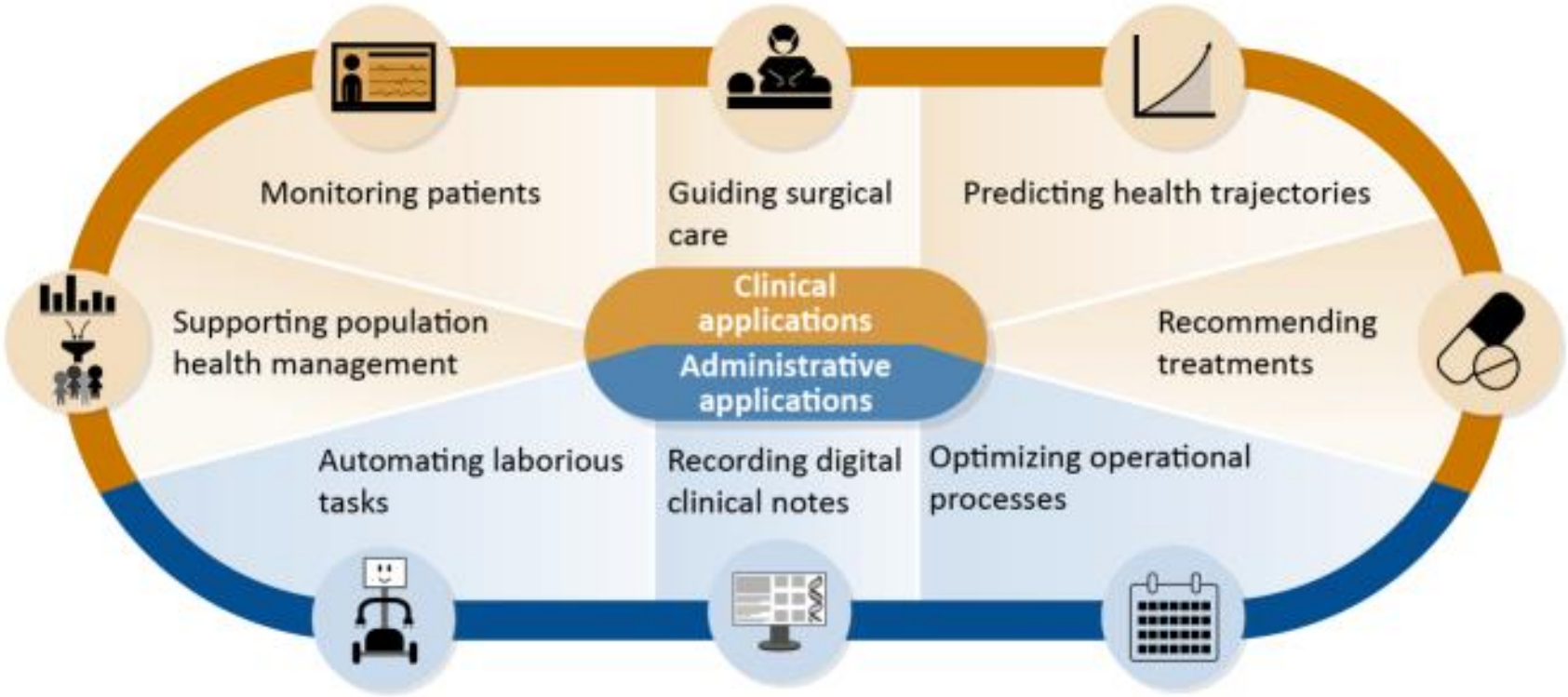
- The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides individuals with several legal, enforceable rights intended to empower them to be more active participants in managing their health information.
- In the HTI-1 Proposed Rule, we made several proposals in support of the HIPAA Privacy Rule's individuals' "right to request a restriction" on certain uses and disclosures of their PHI (*see also* 45 CFR 154.522(a)).

HTI-1 Final Rule

- In the HTI-1 Final Rule, we require support for an "internet-based method" for patients to request a restriction on the use or disclosure of their data in § 170.315(e)(1) (VDT) by 01/01/26.
- Based on feedback received and readiness of the technology, we have decided not to finalize the remainder of the proposals for new criteria.
- We will continue to monitor efforts in the industry related to technological advancement to support patient-requested restrictions.

Decision Support Interventions

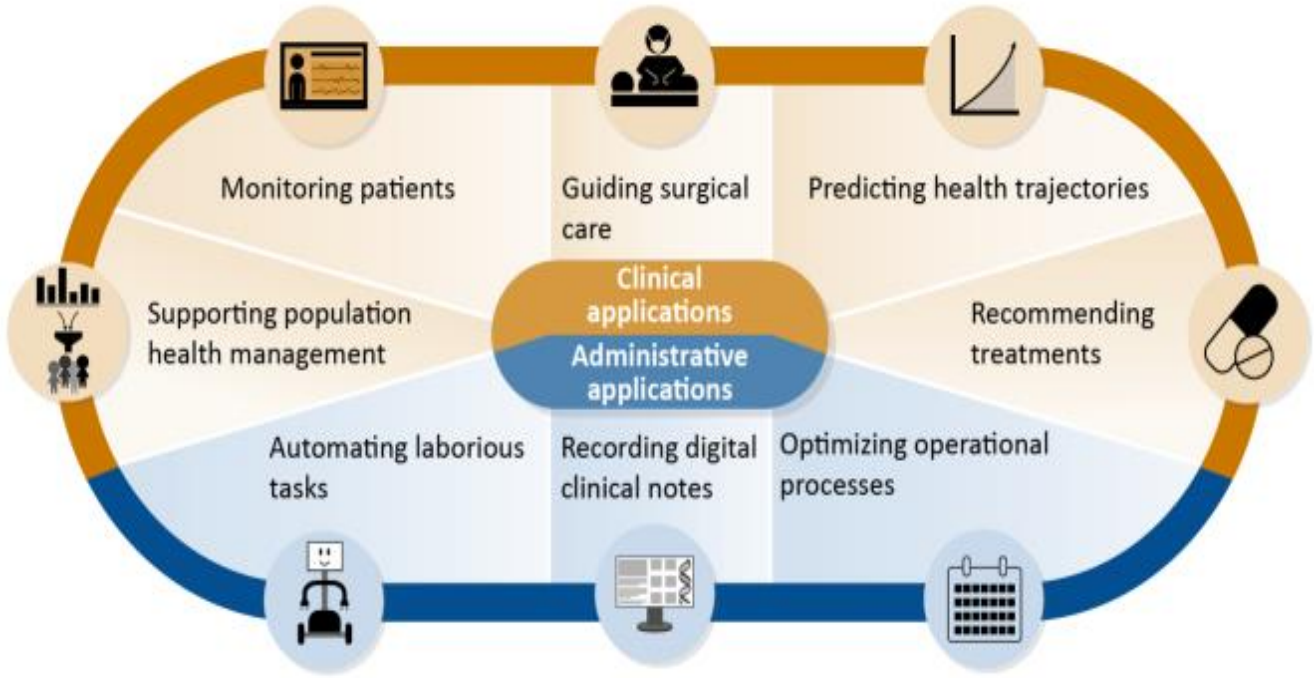
How can AI be used in healthcare?



GAO. | GAO-21-7SP

https://www.gao.gov/assets/gao-21-7sp.pdf

What are the challenges?



GAO. | GAO-21-7SP

- **Amplify** implicit and structural biases
- **Magnify** ethical, legal, and social concerns related to data collection and use
- **Reinforce** common, non-evidence-based practices
- **Solidify** existing inexplicable differences in health outcomes
- **Perpetuate** information asymmetries regarding a model's quality
- **Lead** to recommendations that are ineffective or unsafe

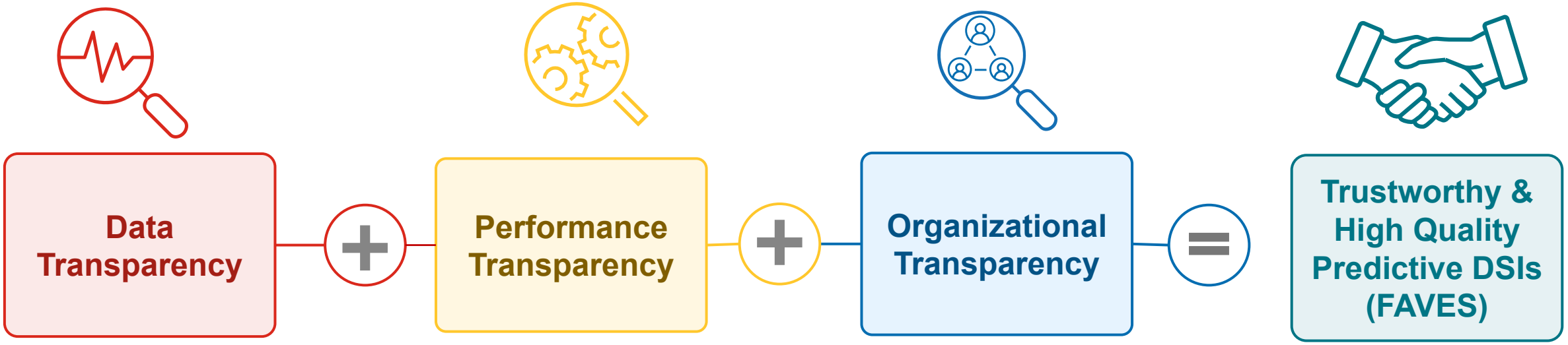
Source: *"Getting the Best out of Algorithms in Health Care." Health IT Buzz blog. June 15, 2022*

An inclusive framing of how to address challenges

FAVES describes the characteristics of “high-quality” algorithms and communicates how we may get the best out of predictive models in health care

- **F**air (unbiased, equitable) - Model does not exhibit biased performance, prejudice or favoritism toward an individual or group based on their inherent or acquired characteristics. The impact of using the model is similar across same or different populations or groups.
- **A**ppropriate - Model is well matched to specific contexts and populations to which it is applied.
- **V**alid - Model has been shown to estimate targeted values accurately and as expected in both internal and external data.
- **E**ffective - Model has demonstrated benefit and significant results in real-world conditions.
- **S**afe – Model use has probable benefits that outweigh any probable risk

ONC's View: Transparency Is a Prerequisite for Trustworthy AI



Data Transparency

Requirements enable users to know when a DSI uses specific data elements relevant to health equity

Performance Transparency

Enable users to have consistent and routine electronic access to technical, and performance information on Predictive DSIs

Organizational Transparency

Requirement for Certified Health IT developers to apply intervention risk management for each Predictive DSI they supply as part of their Health IT Module

Predictive Decision Support Interventions

- ***Predictive Decision Support Intervention or Predictive DSI*** means technology that:
  1. Supports decision-making based on algorithms or models that
  2. Derive relationships from training data and then
  3. Produces an output that results in prediction, classification, recommendation, evaluation, or analysis

- The ONC Definition for Predictive DSI is
  - **Broad in scope:** includes a variety of techniques from algebraic equations to machine learning from relatively simple risk calculators (ASCVD or APACHE IV) to deep neural networks and LLMs
  - **Use case inclusive:** clinical, payer, research, administrative use cases
  - **Risk independent:** high-risk, low-risk, unknown risk
  - **Developer agnostic:** certified EHR company, health system, academic research lab, consumer technology firm

Is my technology or function a Predictive DSI?

ONC does not make determinations regarding whether a specific function or technology constitutes an evidence-based or predictive decision support intervention. Certified Health IT Developers should refer to the regulatory definition of "Predictive Decision Support Intervention" at 45 CFR 170.102 and the regulatory descriptions of evidence-based decision support interventions described in the HTI-1 Final Rule preamble, especially discussion beginning at 89 FR 1241. ONC encourages Certified Health IT Developers and other interested parties to make their own determinations about whether a specific function or technology constitutes a decision support intervention for purposes of compliance with 45 CFR 170.315(b)(11) under the Certification Program. We note that several examples of both Predictive DSIs and non-Predictive (i.e., evidence-based) DSIs are provided in the HTI-1 Final Rule preamble at 89 FR 1245, and we provide several additional clarifications and examples of different DSI types across section III.C.5 of the HTI-1 Final Rule.

When is a developer responsible for source attribute content and risk management practices?

- Is the Predictive DSI supplied by the certified health IT developer?
  - Yes = Source attribute information must be complete and up-to-date and risk management practices must be applied
  - No = No requirements for source attribute information/content but source attribute categories must still be available for customers to use
    - Customers must be able to select a Predictive DSI that they self-develop or that they want to use from a third/other party
    - No requirements to apply risk management practices
- There are no requirements for customers that self-develop or purchase from a third party a Predictive DSI to provide source attribute information to their certified health IT developer
  - Unless that Predictive DSI is subsequently supplied by the developer of certified health IT as part of its Health IT Module

Reduced configuration nexus for Predictive DSIs & Health IT Modules

Finalized Configuration Nexus for § 170.315(b)(11)

"Supplied by the health IT developer as part of its Health IT Module"

- Includes Predictive DSIs that are authored or developed by the certified health IT developer
- Includes Predictive DSIs that are authored or developed by other parties if those Predictive DSIs are sold, marketed, or otherwise explicitly included as part of a Health IT Module
- Supplied by means that
  - Certified health IT developer has taken on stewardship and accountability for that Predictive DSI for the purposes of the Health IT Module
  - Knowledge of its use is known by the Certified Health IT developer

ONC requirements in action: An analogy

NES EHR

NES-developed Hypertension Predictive Model

NES EHR *Now With*: Zelda's Hypertension Predictive Model

What about Konami's Contra-indications Model?

Predictive DSIs authored, developed, or supplied by a Certified Health IT developer are subject to ONC requirements

Made by third-party for NES EHR

Developers are not required to author, develop, or supply a Predictive DSI to be certified

And / Or

No Predictive DSI authored, developed, or supplied by developer of certified health IT

13 Source Attributes for Evidence-based DSIs

Already required as part of CDS criterion

1. **Bibliographic Information**
2. **Developer of the intervention**
3. **Funding source of the technical implementation for the intervention's development**
4. **Release, an if applicable, revision date(s) of the intervention**

Use of data elements salient to health equity

5. **Use of race in the intervention**
6. **Use of ethnicity in the intervention**
7. **Use of language in the intervention**
8. **Use of sexual orientation in the intervention**
9. **Use of gender identity in the intervention**
10. **Use of sex in the in the intervention**
11. **Use of age (date of birth) in the intervention**
12. **Use of social determinants of health in the intervention**
13. **Use of health status assessments data in the intervention**

Nine Predictive DSI Source Attribute Categories

1. Details and output of the intervention
2. Purpose of the intervention
3. Cautioned Out-of-Scope Use of the intervention
4. Intervention development details and input features
5. Process used to ensure fairness in development of the intervention
6. External validation process
7. Quantitative measures of performance
8. Ongoing maintenance of intervention implementation and use
9. Update and continued validation or fairness assessment schedule

Thirty-One Predictive DSI Source Attributes

1 General Description and Outputs

1) Name and contact information for the intervention developer;
2) Funding source of the technical implementation for the intervention(s) development;
3) Description of value that the intervention produces as an output; and
4) Whether the intervention output is a prediction, classification, recommendation, evaluation, analysis, or other type of output.

2 Purpose

5) Intended use of the intervention;
6) Intended patient population(s) for the intervention's use;
7) Intended user(s); and
8) Intended decision-making role for which the intervention was designed to be used/for.

3 Cautioned Out-of-Scope Use

9) Description of tasks, situations, or populations where a user is cautioned against applying the intervention; and
10) Known risks, inappropriate settings, inappropriate uses, or known limitations.

4 Development and Input Features

11) Exclusion and inclusion criteria that influenced the data set;
12) Use of variables in paragraph (b)(11)(iv)(A)(5)-(13) as input features;
13) Description of demographic representativeness including, at a minimum, those used as input features in the intervention;
14) Description of relevance of training data to intended deployed setting;

5 Process used to ensure fairness

15) Description of the approach the intervention developer has taken to ensure that the intervention's output is fair; and
16) Description of approaches to manage, reduce, or eliminate bias.

6 External Validation Process*

17) Description of the data source, clinical setting, or environment where an intervention's validity and fairness has been assessed, other than the source of training and testing data
18) Party that conducted the external testing;
19) Description of demographic representativeness of external data including, at a minimum, those used as input features in the intervention;
20) Description of external validation process.

7 Quantitative Measures of Performance

21) Validity of intervention in test data derived from the same source as the initial training data;
22) Fairness of intervention in test data derived from the same source as the initial training data;
23) Validity of intervention in data external to or from a different source than the initial training data;*
24) Fairness of intervention in data external to or from a different source than the initial training data;*
25) References to evaluation of use of the intervention on outcomes, including, bibliographic citations or hyperlinks to evaluations of how well the intervention reduced morbidity, mortality, length of stay, or other outcomes;*

8 Ongoing Maintenance of Intervention

26) Description of process and frequency by which the intervention's validity is monitored over time;
27) Validity of intervention in local data;*
28) Description of the process and frequency by which the intervention's fairness is monitored over time.
29) Fairness of intervention in local data;* and

9 Validation or Fairness Schedule*

30) Description of process and frequency by which the intervention is updated; and
31) Description of frequency by which the intervention's performance is corrected when risks related to validity and fairness are identified.

Scope of DSIs considered evidence-based for purposes of the Program

- Enable a user to provide electronic feedback data for **evidence-based decision support interventions** and make available such feedback data, in a computable format, including at a minimum the intervention, action taken, user feedback provided (if applicable), user, date, and location

- For purposes of requirements in § 170.315(b)(11), we finalized that evidence-based DSIs are limited to only those DSIs that
  - Are actively presented to users in clinical workflow to enhance, inform, or influence decision-making related to the care a patient receives
- This has implications for DSIs that Health IT Modules must
  - Enable selection (i.e. activation) of
  - Enable users to access source attributes for
  - Support “feedback loop” functionality for

Organizational transparency on risk management of Predictive DSIs

Intervention risk management practices must be applied for each Predictive DSI supplied by the health IT developer as part of its Health IT Module

1. Validity
2. Reliability
3. Robustness
4. Fairness
5. Intelligibility
6. Safety
7. Security
8. Privacy

- Predictive DSI(s) must be subject to
  - Analysis of potential risks and adverse impacts
  - Practices to mitigate identified risks
  - Policies and implemented controls for governance, including how data are acquired, managed, and used
- Final Rule preamble describes each characteristic and associated approaches that can be taken to assess and mitigate risks
  - Note: many of the terms and concepts in the IRM requirements rely on the National Institute of Standards and Technology (NIST) AI Risk Management Framework
- Summary information of risk management and governance to be publicly available

Assurances Condition and Maintenance of Certification requirements

- Finalized a DSI criterion-specific instantiation of general Certification Program expectations as new Maintenance of Certification Requirements
- Builds on three specific existing Assurances Condition of Certification requirements
- Establishes ongoing obligations for developers of certified health IT that supply Predictive DSIs as part of their Health IT Modules to
  - Enable user access to updated descriptions of source attribute information
  - Review and update as necessary IRM practices that must be applied for each Predictive DSI the health IT developer supplies as part of its Health IT Module
  - Ensure the ongoing public accessibility of updated summary IRM practice information as submitted to their ONC-ACB via hyperlink
- Recognizes that such ongoing requirements would best fit under the Program as a developer-level responsibility, rather than a product-level responsibility

Implementation Timeline & requirements

Health IT Developers

- Will have one year to update their certified health IT to support capabilities in 170.315(b)(11)
- Will need to provide updated technology to their customers by December 31, 2024
- Will need to provide summary IRM practice information to their ONC-ACB before December 31, 2024
- Will need to keep source attribute information and risk management information up-to-date as an ongoing maintenance of certification requirement
- Will need to include as part of Real World Testing Plans and Results

Providers

- As of their 2025 performance period for CMS payment policy, certified health IT will support providers' ability to access and modify detailed source attribute information for evidence-based and Predictive DSIs they use

Industry

- The 31 source attributes finalized offers an industry-wide baseline from which more detailed "model cards" and other industry consensus can be formed
- Transparency provisions are likely to incentivize the creation and support of fairer, better validated algorithms in healthcare

Insights Condition and Maintenance of Certification

The Cures Act laid the foundation for transparent reporting:

- Established the requirement to create an Electronic Health Record (EHR) Reporting Program to provide transparent reporting to measure the performance of certified health IT
- Specified its implementation as part of a Condition and Maintenance of Certification for developers of certified health IT

Insights Condition provides transparent reporting that:

- Addresses information gaps in the health IT marketplace
- Provides insights on the use of specific certified health IT functionalities
- Provides information about consumers' experience with certified health IT

Insights Condition: Measures and Related Criteria

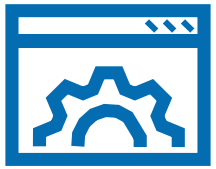
AREA	MEASURE	RELATED CRITERION/CRITERIA
Individuals' Access to EHI	Individuals' Access to Electronic Health Information Through Certified Health IT	§§ 170.315(e)(1) and (g)(10)
Clinical Care Information Exchange	C-CDA Problems, Medications, and Allergies Reconciliation and Incorporation Through Certified Health IT	§ 170.315(b)(2)
Standards Adoption & Conformance	Applications Supported Through Certified Health IT	§ 170.315(g)(10)
Standards Adoption & Conformance	Use of FHIR in Apps Through Certified Health IT	§ 170.315(g)(10)
Standards Adoption & Conformance	Use of FHIR Bulk Data Access Through Certified Health IT	§ 170.315(g)(10)
Public Health Information Exchange	Immunization Administrations Electronically Submitted to Immunization Information Systems Through Certified Health IT	§ 170.315(f)(1)
Public Health Information Exchange	Immunization History and Forecasts Through Certified Health IT	§ 170.315(f)(1)

Note: Metrics associated with the measures are described in the measure specification sheets published on ONC's website.

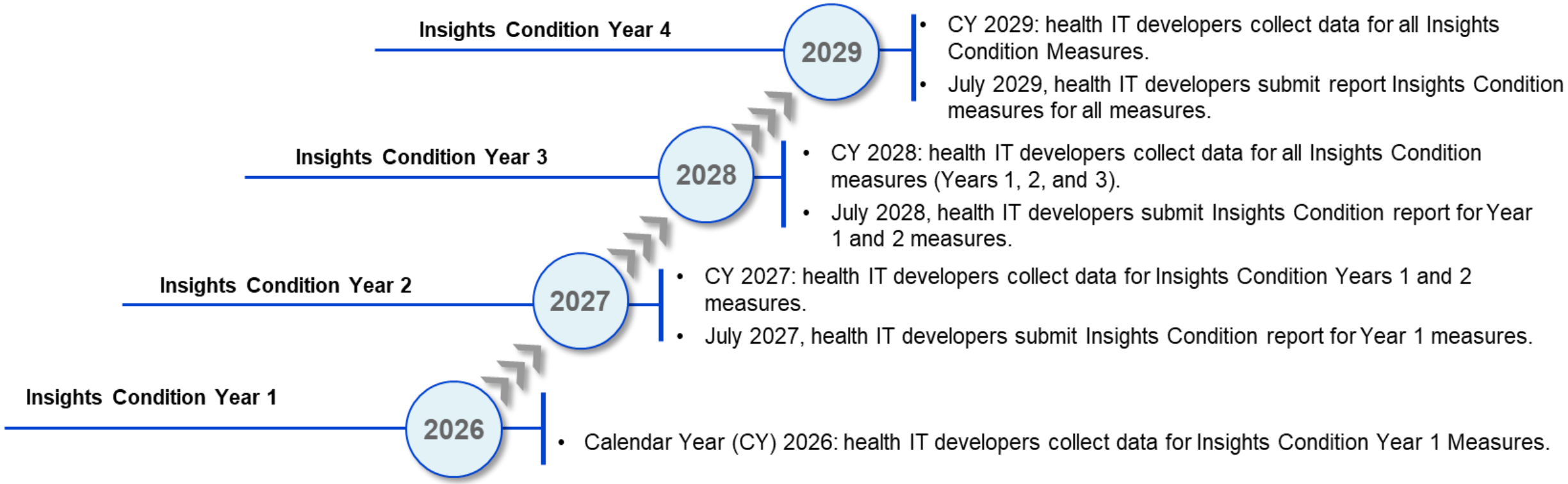
Who Will Be Reporting on These Measures and How?

- Developers of certified health IT must submit responses if the developer meets each of the following criteria:
  - Has at least 50 hospital sites or 500 individual clinician users across their certified health IT;
  - Has any health IT certified to the certification criteria specified in each measure; and
  - Has any users using the certified health IT associated with the measure.

- Developers of certified health IT who do not meet the qualifications above will submit a response (attestation) to indicate that they do not meet the minimum reporting qualifications for a measure.

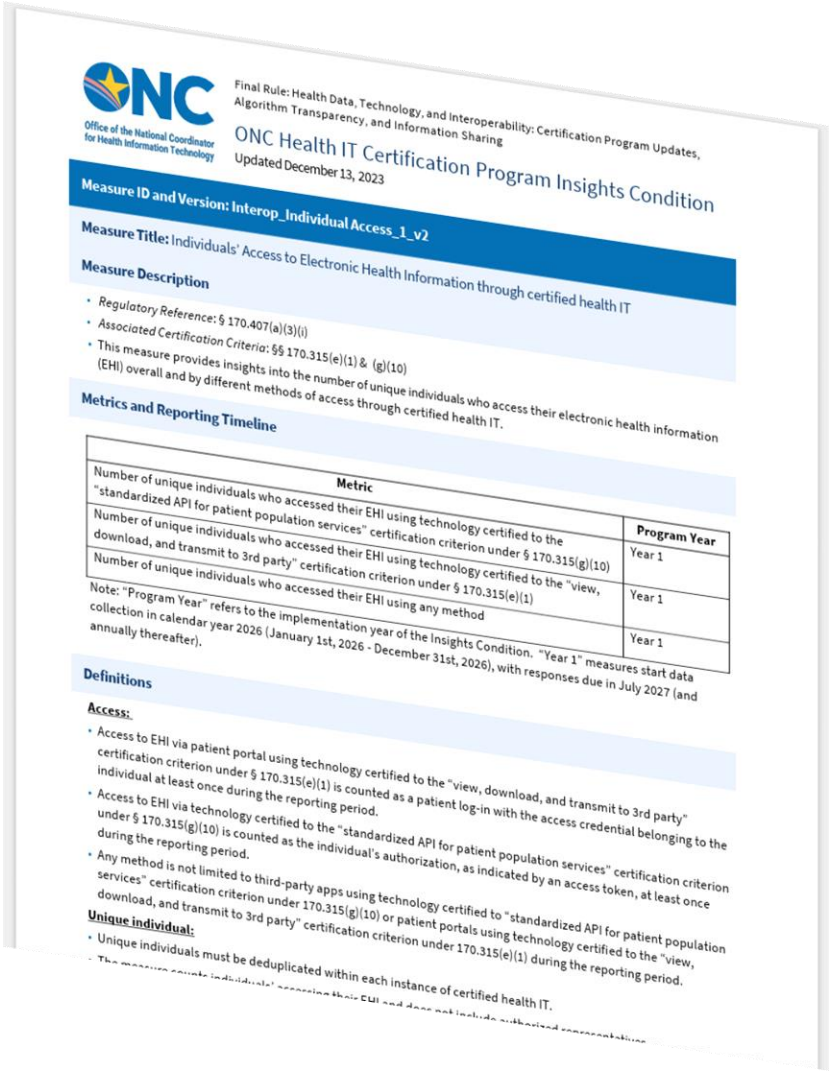


What Is the Reporting Timeline?



Resources to Understand Measures and Metrics

- Current Resource: Measure Specification Sheets
  - Each measure has a set of metrics associated with it that will be reported.
  - Measure specification sheets detail the metrics, provide definitions and provide guidance on implementing the measure.
  - The specification sheets can be found here:
  - https://healthIT.gov/HTI-1



ONC
Office of the National Coordinator for Health Information Technology

Final Rule: Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing

ONC Health IT Certification Program Insights Condition

Updated December 13, 2023

Measure ID and Version: Interop_Individual Access_1_v2

Measure Title: Individuals' Access to Electronic Health Information through certified health IT

Measure Description

- *Regulatory Reference*: § 170.407(a)(3)(i)
- *Associated Certification Criteria*: §§ 170.315(e)(1) & (g)(10)
- This measure provides insights into the number of unique individuals who access their electronic health information (EHI) overall and by different methods of access through certified health IT.

Metrics and Reporting Timeline

Metric	Program Year
Number of unique individuals who accessed their EHI using technology certified to the "standardized API for patient population services" certification criterion under § 170.315(g)(10)	Year 1
Number of unique individuals who accessed their EHI using technology certified to the "view, download, and transmit to 3rd party" certification criterion under § 170.315(e)(1)	Year 1
Number of unique individuals who accessed their EHI using any method	Year 1

Note: "Program Year" refers to the implementation year of the Insights Condition. "Year 1" measures start data collection in calendar year 2026 (January 1st, 2026 - December 31st, 2026), with responses due in July 2027 (and annually thereafter).

Definitions

Access:

- Access to EHI via patient portal using technology certified to the "view, download, and transmit to 3rd party" certification criterion under § 170.315(e)(1) is counted as a patient log-in with the access credential belonging to the individual at least once during the reporting period.
- Access to EHI via technology certified to the "standardized API for patient population services" certification criterion under § 170.315(g)(10) is counted as the individual's authorization, as indicated by an access token, at least once during the reporting period.
- Any method is not limited to third-party apps using technology certified to "standardized API for patient population services" certification criterion under 170.315(g)(10) or patient portals using technology certified to the "view, download, and transmit to 3rd party" certification criterion under 170.315(e)(1) during the reporting period.

Unique individual:

- Unique individuals must be deduplicated within each instance of certified health IT.

Feedback led to changes to the reporting process…

More Time and Reduced Reporting

- Delayed start date for collecting and reporting measures
- Spreading the implementation of the measures across 3 years instead of 2 years
- Reduced reporting from twice a year to annually
- Insights measures can be re-used for meeting RWT reporting requirements

CHPL HTI-1 Features

Jim Younkin

Roxanne Johanning

CHPL HTI-1 Functionality

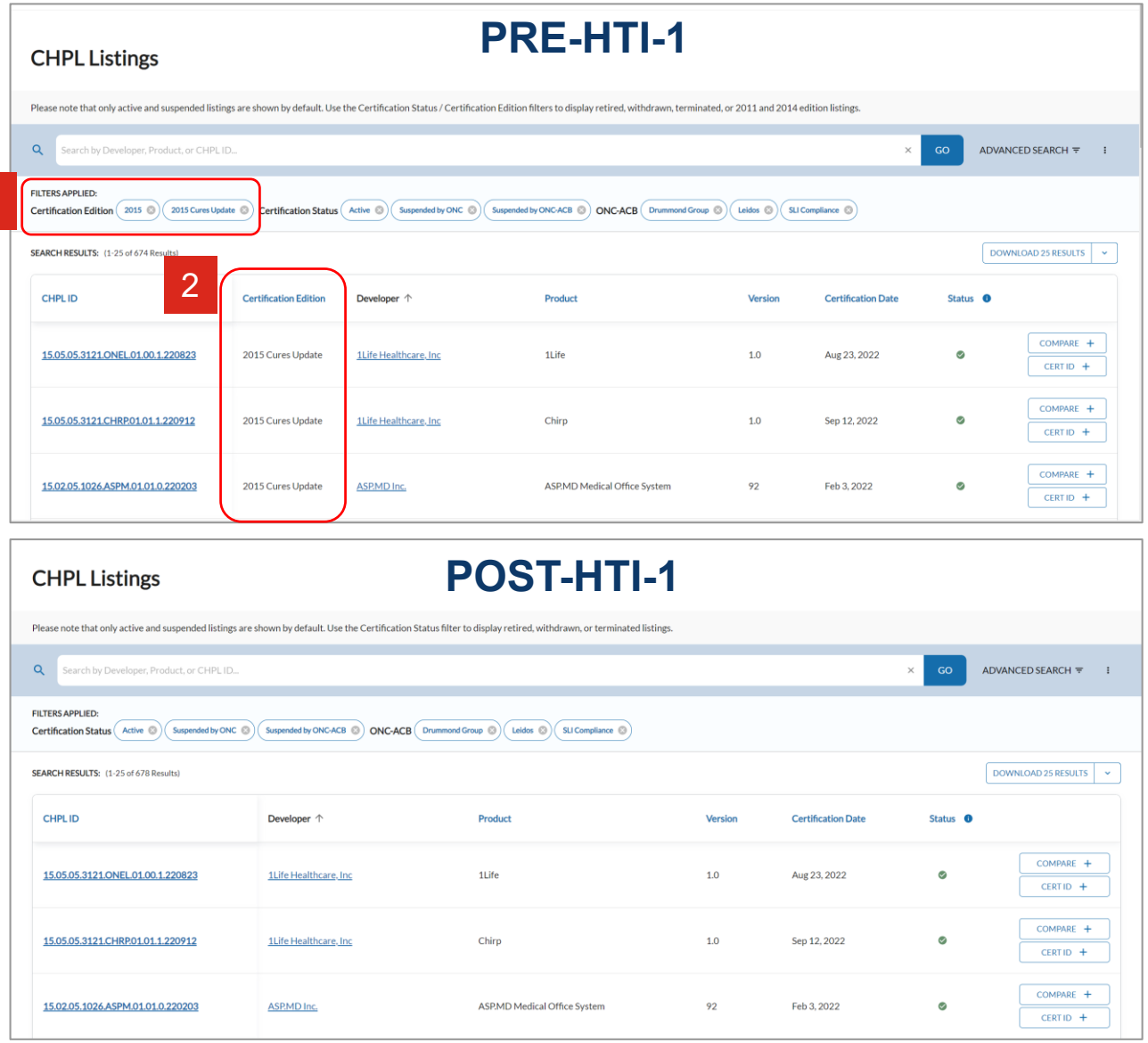
- Replaced edition-based functionality with Editionless
- Removed “Edition” and “Cures Update”
- Added “Standards” and “Functionality Tested” to Listing Details

CHPL HTI-1 Functionality Changes for Everyone

1. Removed “Certification Edition” from Search and Listing View Details
2. Added Standards to Listing Details
3. Added Indicators to Standards and Functionality Tested based on Dates
   -  “Update Needed” – Update is required by a future date
   -  “Requirement Met” – Met a requirement before its required date
   -  “Requirement Not Met” – A requirement was not met by its required date

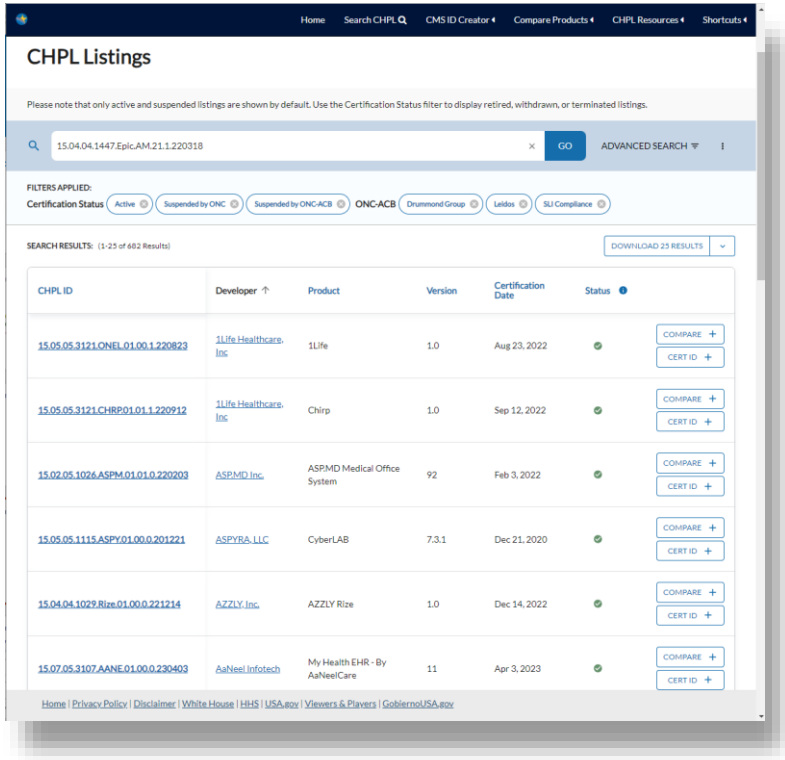
PRE/POST HTI-1 Screenshots – Search Filter/Results

1. Removed Certification Edition Filters
2. Removed Certification Edition column

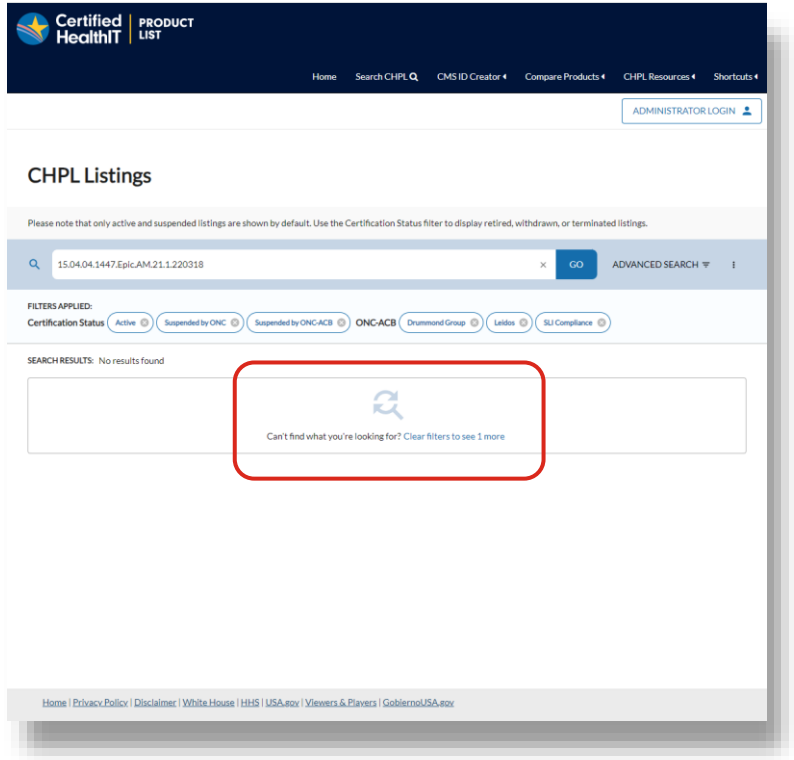


CHPL Search Feature: “Can’t find what you’re looking for?”

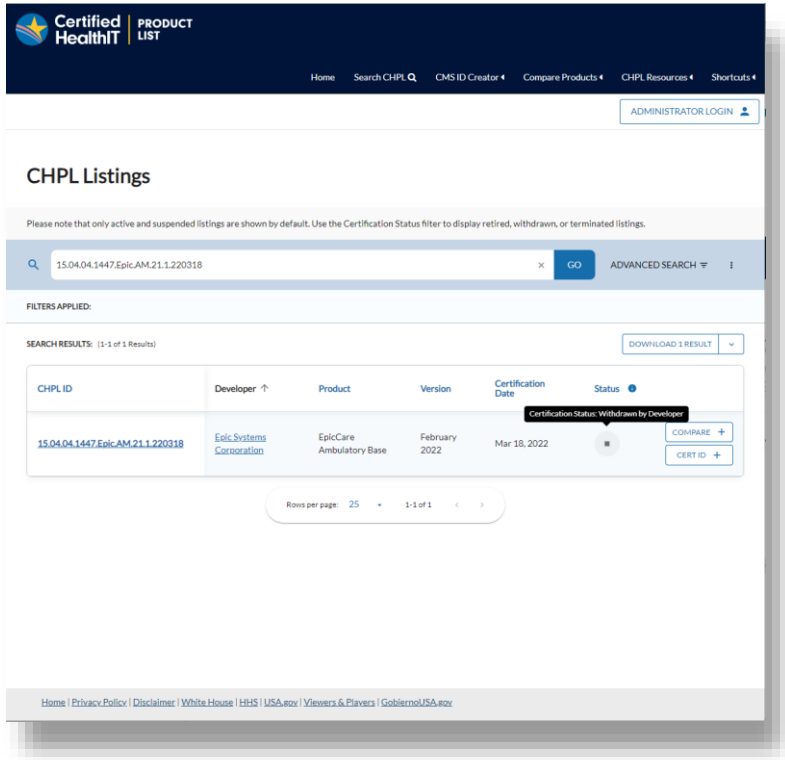
Enter a Withdrawn or Retired Listing



No Results Found



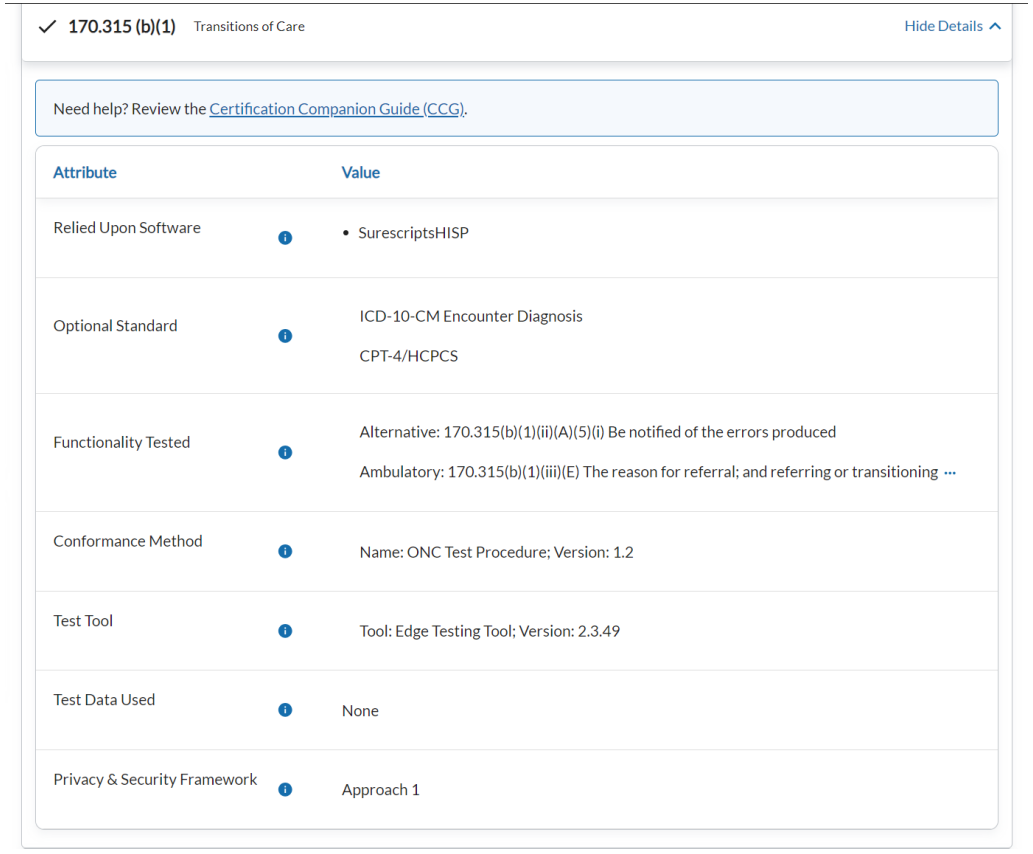
Additional Results Returned



**“Can’t find what you’re looking for?
Clear filters to see __ more”**

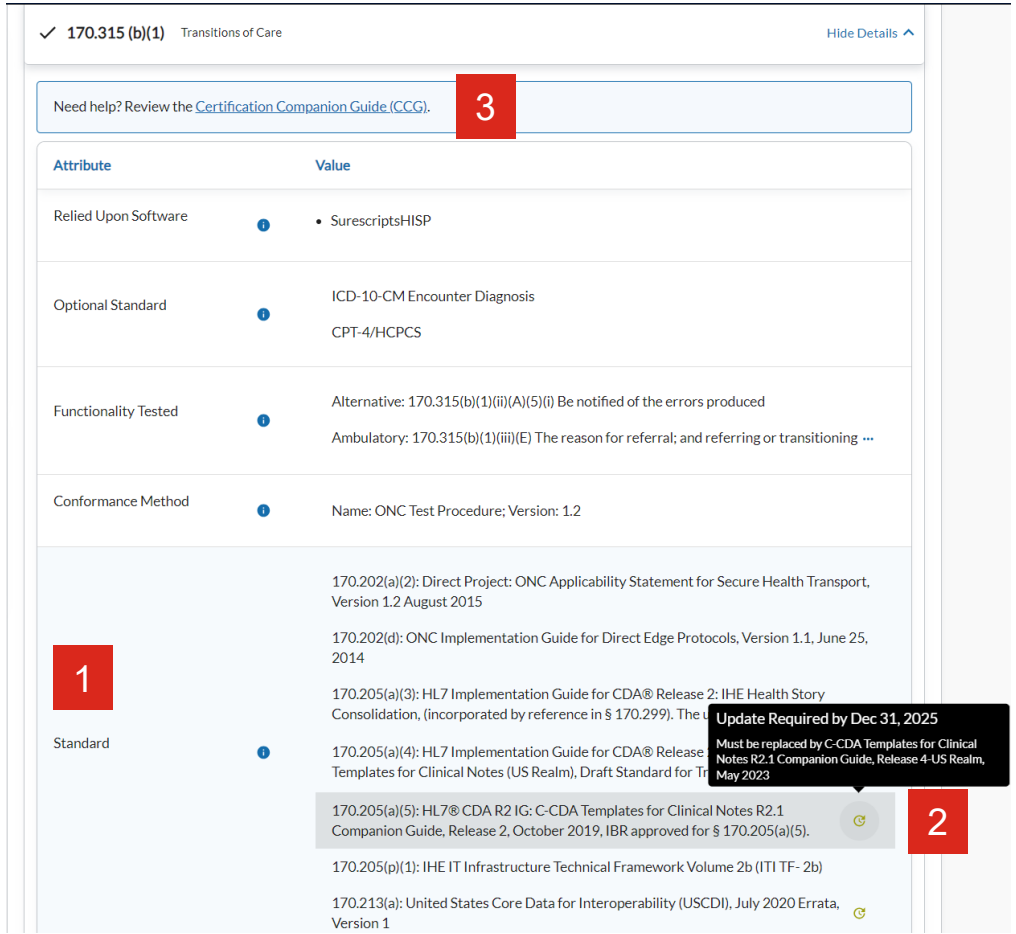
PRE/POST HTI-1 Screenshots – Listing Details

PRE-HTI-1



1. New "Standards" Attribute
2. Indicators to show status of Standards requiring updates
3. Link to CCG*

POST-HTI-1



* Recently added to production to provide easy access to certification information

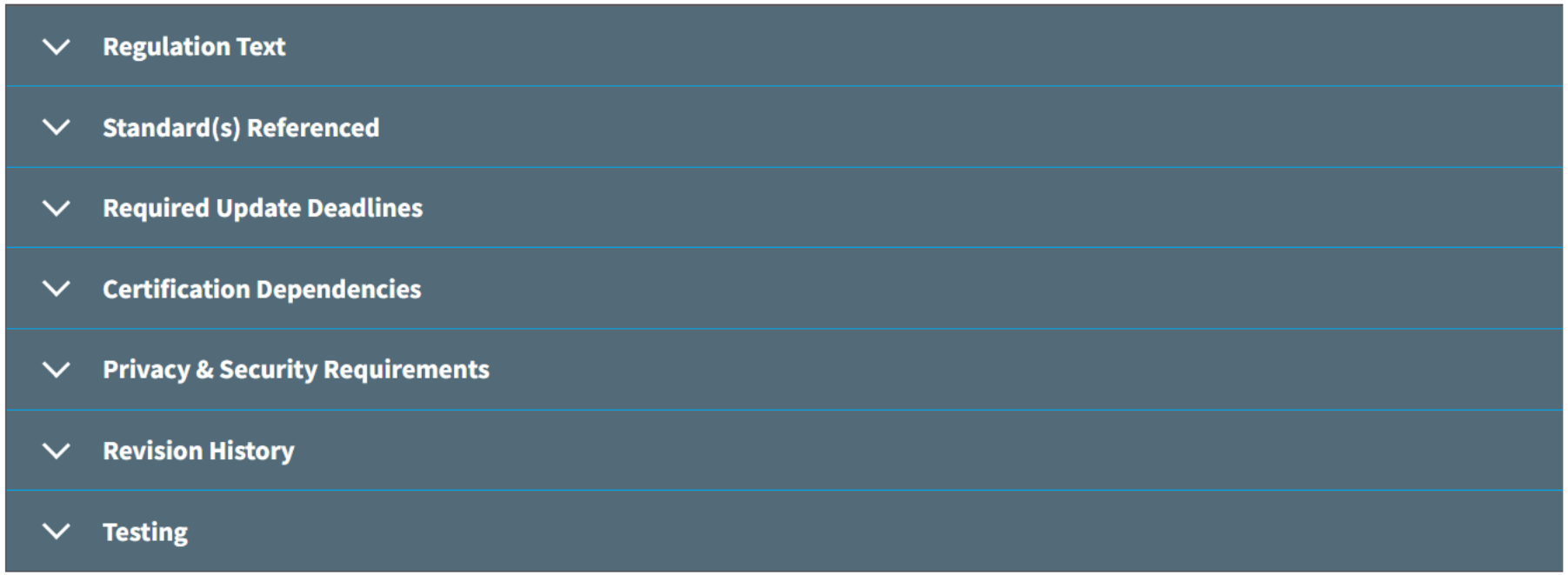
Test Procedure and CCG Layout Updates

Ashley Hain

Summary of Changes

1. Updated Accordions added across CCGs and TPs
2. Updates to the CCG Table
3. New dropdowns for TP requirements dependent on expiration/required dates

Accordion Updates



New accordion sections added across criteria. These accordions will only appear if there are requirements/content available for a respective criteria.

Removed “Resource Document” accordion. Resources included there are now embedded within relevant sections of CCGs/TPs and/or included on the Program Resources page.

Required Update Deadlines

Required Update Deadlines

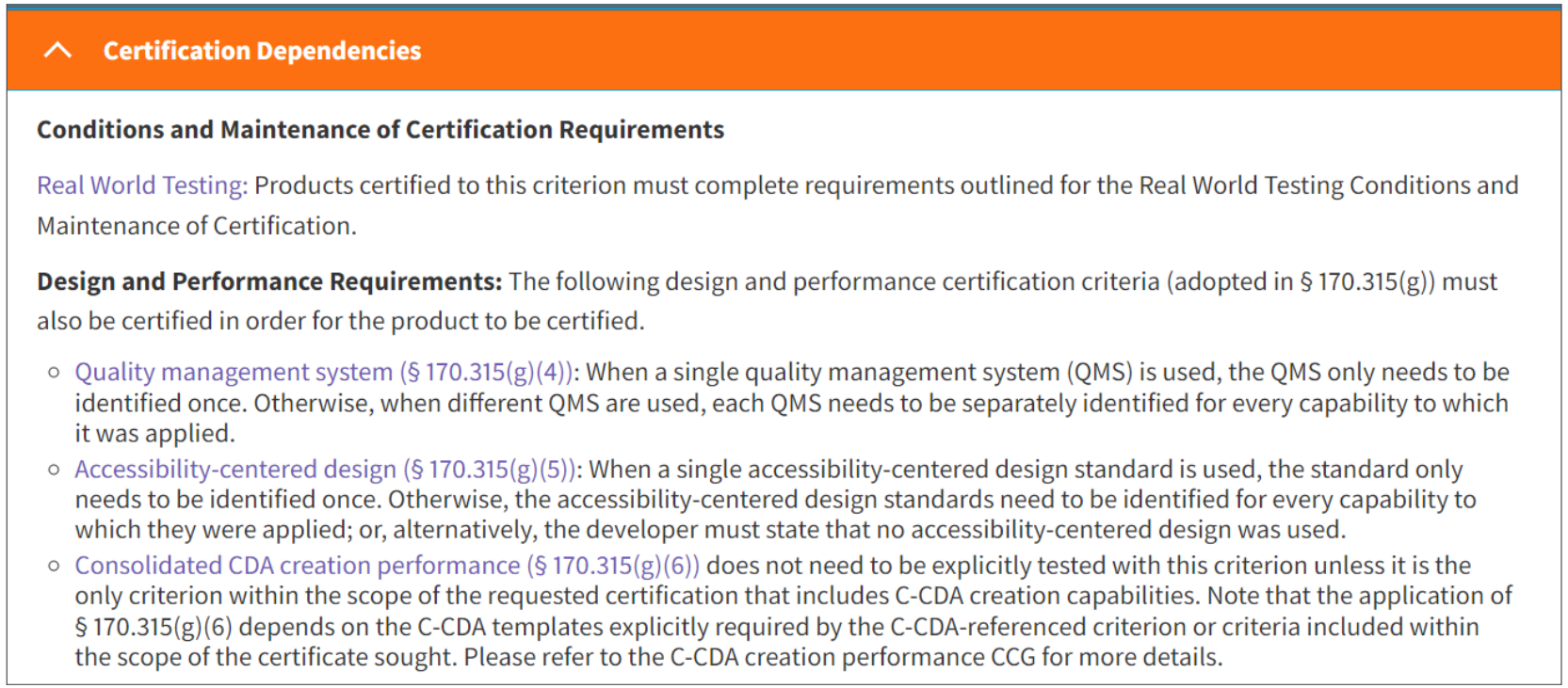
The following outlines deadlines for required updates for this criterion as they relate to changes published in recent ONC final rules. Developers must update their products to the requirements outlined and provide them to their customers by the stated deadlines. These represent one-time deadlines as set by recent regulatory updates and do not encompass ongoing deadlines related to the Conditions and Maintenance of Certification. Please review those requirements for additional compliance activities related to one's certification under Certification Dependencies.

Deadline: December 31, 2025

Action to be taken: Developers certified to this criterion must update their use of standards and minimum standard code sets outlined in paragraphs (b)(1)(ii) and (b)(1)(iii)(A)-(F). Developers must add functionality certified to the standards referenced in paragraphs (b)(1)(iii)(A)-(F).

- This accordion summarizes the major requirements for updates and associated deadlines for these updates.
- It is not intended to provide all details related to an update, but instead give the developer an understanding of what they may need to consider if certified to that criterion.

Certification Dependencies



Certification Dependencies

Conditions and Maintenance of Certification Requirements

Real World Testing: Products certified to this criterion must complete requirements outlined for the Real World Testing Conditions and Maintenance of Certification.

Design and Performance Requirements: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- Quality management system (§ 170.315(g)(4)): When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, when different QMS are used, each QMS needs to be separately identified for every capability to which it was applied.
- Accessibility-centered design (§ 170.315(g)(5)): When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively, the developer must state that no accessibility-centered design was used.
- Consolidated CDA creation performance (§ 170.315(g)(6)) does not need to be explicitly tested with this criterion unless it is the only criterion within the scope of the requested certification that includes C-CDA creation capabilities. Note that the application of § 170.315(g)(6) depends on the C-CDA templates explicitly required by the C-CDA-referenced criterion or criteria included within the scope of the certificate sought. Please refer to the C-CDA creation performance CCG for more details.

- This accordion captures details as to whether the criterion has related requirements within the Conditions and Maintenance of Certification and/or design and performance related requirements for certification.

- It will present criterion-specific requirements outlined in the Conditions and Maintenance of Certification. Requirements that span across all criteria (e.g., Attestations and Information Blocking) will not be outlined in this section.

Privacy and Security Requirements

Privacy & Security Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(b)(1). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(b) criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific paragraph (a) criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification. However, exceptions exist for § 170.315(e)(1) "View, download, and transmit to 3rd party (VDT)" and (e)(2) "Secure messaging", which are explicitly stated.

For more information on the approaches to meet these Privacy and Security requirements, please review the Privacy and Security CCG.

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))
  - Auditable events and tamper-resistance (§ 170.315(d)(2))
  - Audit reports (§ 170.315(d)(3))
  - Automatic access time-out (§ 170.315(d)(5))
  - Emergency access (§ 170.315(d)(6))
  - End-user device encryption (§ 170.315(d)(7))
  - Integrity (§ 170.315(d)(8))
  - Encrypt authentication credentials (§ 170.315(d)(12))
  - Multi-factor authentication (MFA) (§ 170.315(d)(13))
- If choosing Approach 2:
  - For each applicable privacy and security certification criterion not certified for Approach 1, the health IT developer may certify using system documentation that is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

This accordion captures details as to whether the criterion has requirements as outlined under the privacy and security framework as defined at § 170.550(h).

Version History

Revision History

Version #	Description of Change	Version Date
1.0	Initial publication	03-11-2024

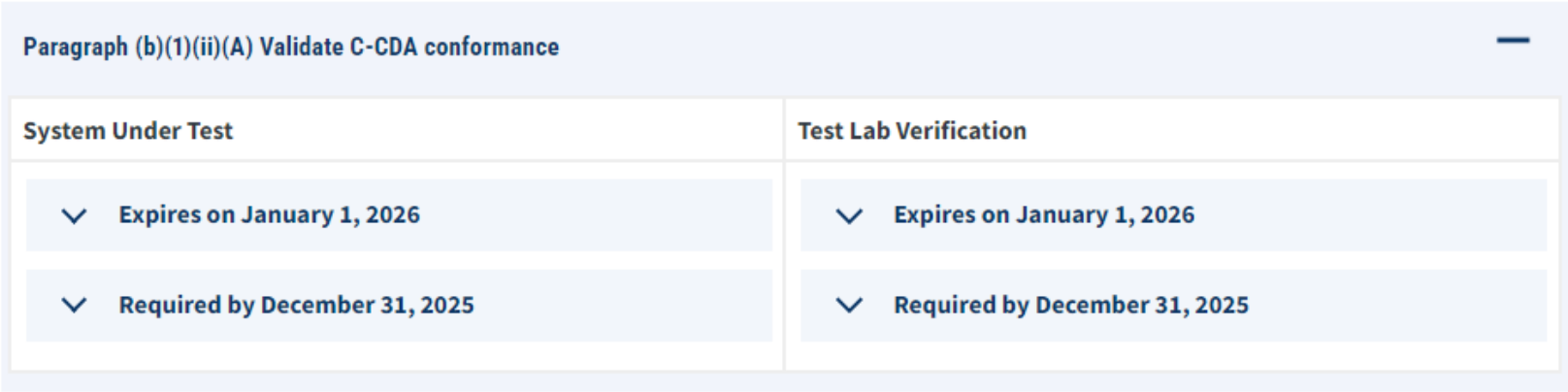
- Versions previously would reset at the start of a new edition.
- Moving forward, all criteria have been reset to 1.0 and will incrementally increase following a two-digit versioning scheme.
  - First digit: Major version when new Final Rule introduces changes to the criterion requirements.
  - Second digit: Minor version when a clarification is made to the CCG or an edit is made to a Test Procedure.

CCG Table Updates

Base EHR Definition	Real World Testing	Insights Condition	SVAP	Requires Updates
Included	Yes	No	Yes	Yes

1. Added Insights Condition and Requires Updates to the table within the CCG.
2. Hyperlinks added to headers for users to obtain more information on the requirements
   - Insights Condition CCG will be hyperlinked when available.

Test Procedure Drop Down Selections



- When Final Rule edits alter a criterion's requirement, affected test steps are split into two to differentiate the changes in requirements.
- Test steps under "Expires on [blank]" will display test steps to achieve the status quo of certification requirements, for which any existing certification should already comply, and will be replaced by updated/new requirements by a specified deadline.
- Test steps under "Required by [blank]" will display test steps for the updated/new requirements to which a Health IT Module must comply by a specified deadline.
- If there are no changes to a subparagraph's requirements, these expandable sections will not be included in the subparagraph.

Office of the National Coordinator for Health Information Technology

Contact ONC

Phone: 202-690-7151

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

Twitter: @onc_healthIT

LinkedIn: Office of the National Coordinator for Health Information Technology

Youtube: https://www.youtube.com/user/HHSONC

HealthIT.gov

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