Standards-based Conformity Assessment of (Software) Products

Lisa Carnahan
Computer Scientist
Standards Services Group
lisa.carnahan@nist.gov

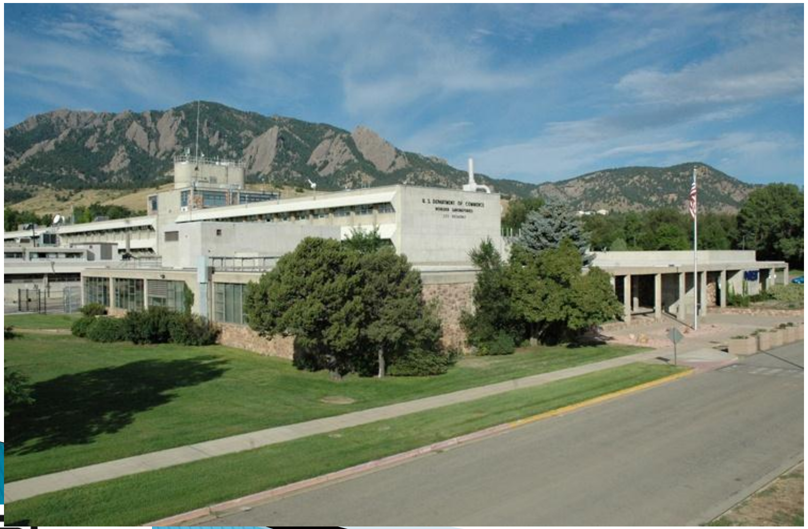
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Agenda

- NIST
- ISO standards for conformity assessment
- Example: three domains
  - HHS EHR Certification Program
  - Cryptographic Module Validation Program
- Product testing handled in a operational context
- Moving forward

US DOC/NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology …



… in ways that enhance economic security and improve our quality of life.

DOC: US Dept of Commerce

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

National Technology Transfer and Advancement Act (NTTAA)

- **Directs US Federal agencies** with respect to their use of private sector standards and conformity assessment practices.
- The objective is for **US Federal agencies to adopt private sector standards, wherever possible,** in lieu of creating proprietary, non-consensus standards.
- **Directs US NIST "to coordinate Federal, State, and local technical standards activities and conformity assessment activities**, with private sector technical standards activities and conformity assessment activities, with the goal of eliminating unnecessary duplication and complexity in the development and promulgation of conformity assessment requirements and measures".
- March 1996

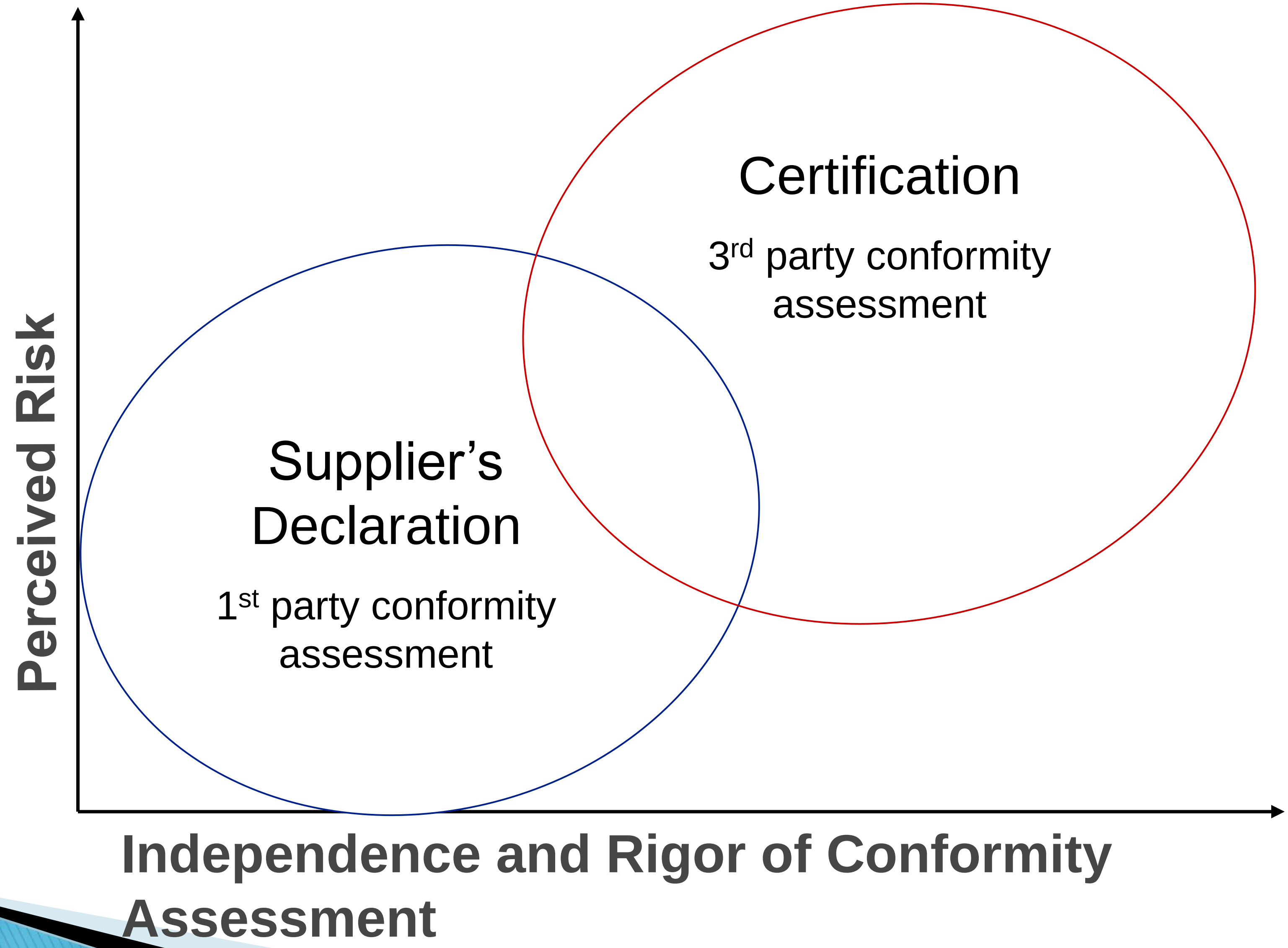
What We Do

- Assist U.S. Federal Government Agencies in developing **conformity** policies and administrative infrastructure
- Design and assist in the implementation of related **conformity assessment** programs
- Develop **test methods and tools** for industry use in standards development and implementation

- Do not operationally test products
- Do not certify products

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Risk and Conformity Assessment-- How Much Confidence is Needed?


Perceived Risk
Certification
3rd party conformity assessment
Supplier's Declaration
1st party conformity assessment
Independence and Rigor of Conformity Assessment

Conformity Assessment

"demonstration that specified requirements relating to a product, process, system, person or body are fulfilled"

ISO/IEC 17000

Typical Use – Certification (3rd Party CA)

- Used when the risks associated with non-conformity are moderate to high
- Includes evaluation, compliance decision, attestation of conformity and some form of *surveillance* or follow up
- Always conducted by a third party
- ISO/IEC Guide 65

Typical Use – Testing (1st, 2nd or 3rd Party CA)

- Used when the critical characteristics can be evaluated via measurement under specified conditions
- Type test is a test carried out on samples that represent production for the purpose of determining conformity
- May be an element of a supplier's declaration or certification system
- ISO/IEC 17025

Typical Use - Accreditation

- Used to assess and ensure/enhance ongoing conformity assessment body and program for competence, management and technical requirements
- Used to attain needed confidence in laboratory testing operation and results
- Used to attain needed confidence in certification system
- ISO/IEC 17011

NVLAP

ANSI
ANSI Accredited Program
PERSONNEL CERTIFICATION

A2LA

The Driver for EHR systems Certification in the US

- American Reinvestment & Recovery Act (ARRA)

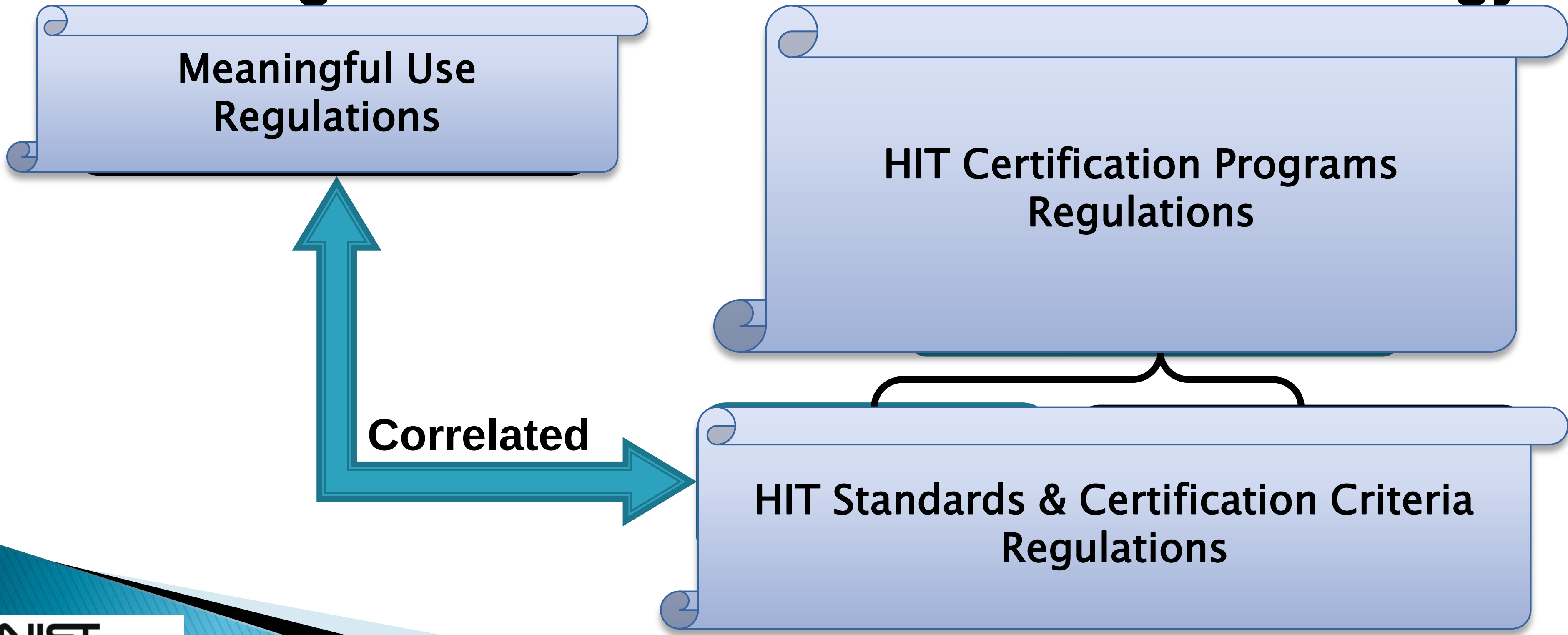
- §3001(c)(5) of the PHSA requires the [**US HHS] National Coordinator** in consultation with the Director of NIST to “keep or recognize a certification program or programs for **the voluntary certification of HIT**… such program shall include, as appropriate, testing… in accordance with §13201(b) of the HITECH Act”

- §13201(b) “…the Director of NIST shall support the establishment of a conformance testing infrastructure… may include a program to accredit independent, non-Federal laboratories to perform testing.”

National Institute of Standards and Technology
U.S. Department of Commerce

How Does All This Work?

“Meaningful User of Certified EHR Technology”



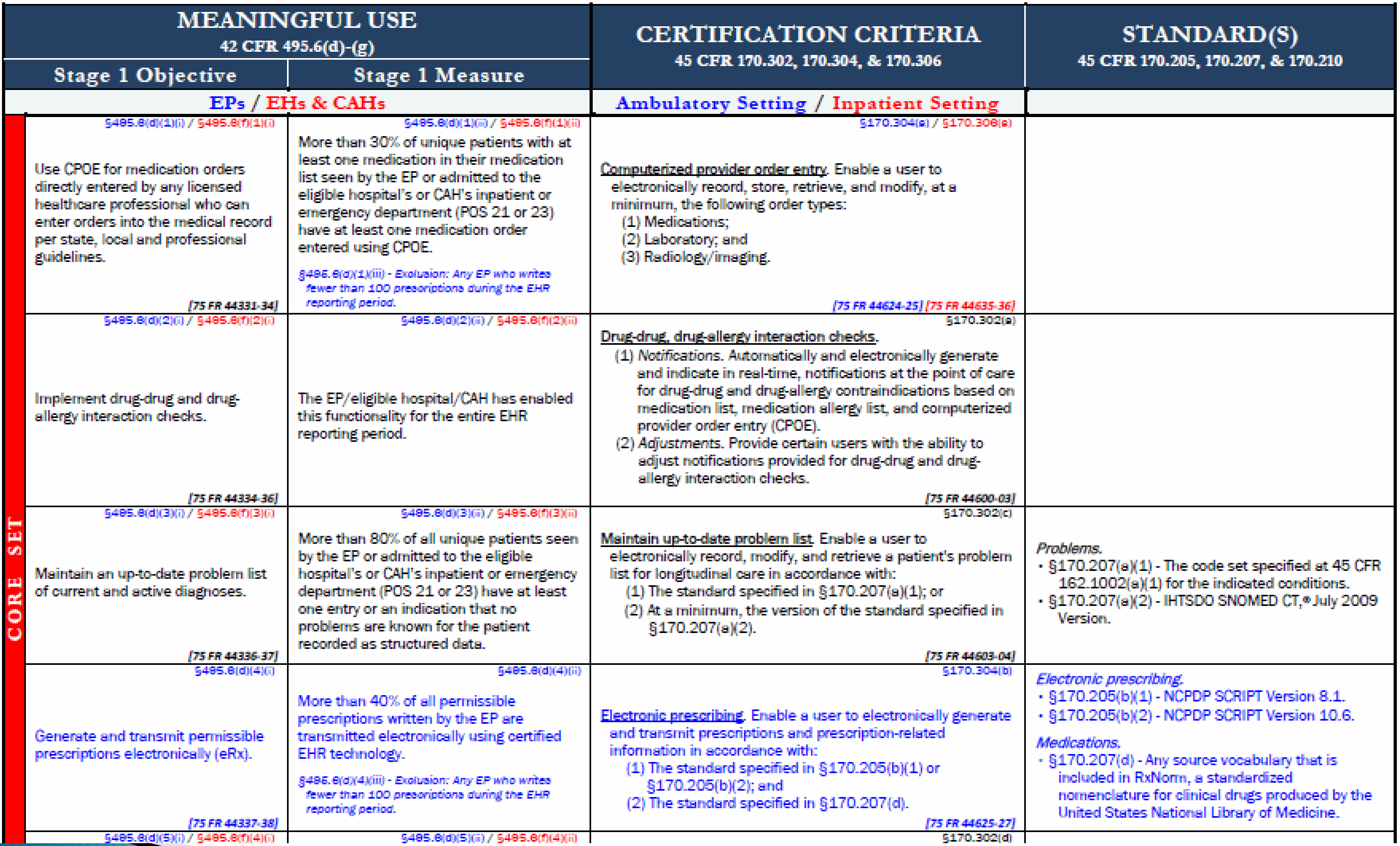
Meaningful Use Regulations

HIT Certification Programs Regulations

Correlated

HIT Standards & Certification Criteria Regulations

MU Criteria & Standards

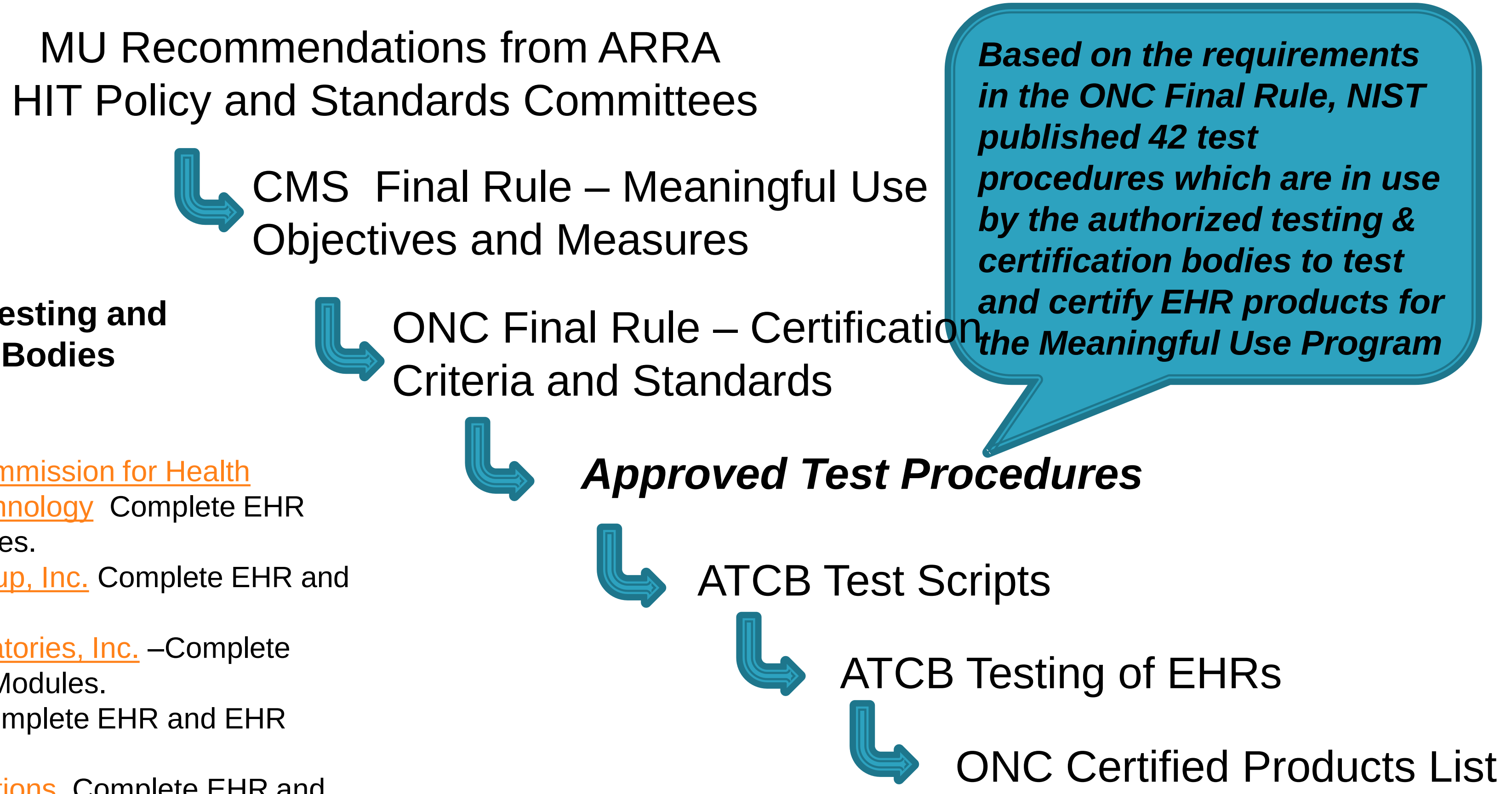


	MEANINGFUL USE 42 CFR 495.6(d)-(g)		CERTIFICATION CRITERIA 45 CFR 170.302, 170.304, & 170.306	STANDARD(S) 45 CFR 170.205, 170.207, & 170.210
	Stage 1 Objective	Stage 1 Measure		
	EPs / EHs & CAHs		Ambulatory Setting / Inpatient Setting	
CORE SET	§495.6(d)(1)(i) / §495.6(f)(1)(i) Use CPOE for medication orders directly entered by any licensed healthcare professional who can enter orders into the medical record per state, local and professional guidelines. *[75 FR 44331-34]*	§495.6(d)(1)(ii) / §495.6(f)(1)(ii) More than 30% of unique patients with at least one medication in their medication list seen by the EP or admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have at least one medication order entered using CPOE. *§495.6(d)(1)(iii) - Exclusion: Any EP who writes fewer than 100 prescriptions during the EHR reporting period.*	§170.304(a) / §170.306(a) Computerized provider order entry. Enable a user to electronically record, store, retrieve, and modify, at a minimum, the following order types: (1) Medications; (2) Laboratory; and (3) Radiology/imaging. *[75 FR 44624-25] [75 FR 44635-36]*	
	§495.6(d)(2)(i) / §495.6(f)(2)(i) Implement drug-drug and drug-allergy interaction checks. *[75 FR 44334-36]*	§495.6(d)(2)(ii) / §495.6(f)(2)(ii) The EP/eligible hospital/CAH has enabled this functionality for the entire EHR reporting period.	§170.302(a) Drug-drug, drug-allergy interaction checks. (1) *Notifications.* Automatically and electronically generate and indicate in real-time, notifications at the point of care for drug-drug and drug-allergy contraindications based on medication list, medication allergy list, and computerized provider order entry (CPOE). (2) *Adjustments.* Provide certain users with the ability to adjust notifications provided for drug-drug and drug-allergy interaction checks. *[75 FR 44600-03]*	
	§495.6(d)(3)(i) / §495.6(f)(3)(i) Maintain an up-to-date problem list of current and active diagnoses. *[75 FR 44336-37]*	§495.6(d)(3)(ii) / §495.6(f)(3)(ii) More than 80% of all unique patients seen by the EP or admitted to the eligible hospital's or CAH's inpatient or emergency department (POS 21 or 23) have at least one entry or an indication that no problems are known for the patient recorded as structured data.	§170.302(c) Maintain up-to-date problem list. Enable a user to electronically record, modify, and retrieve a patient's problem list for longitudinal care in accordance with: (1) The standard specified in §170.207(a)(1); or (2) At a minimum, the version of the standard specified in §170.207(a)(2). *[75 FR 44603-04]*	*Problems.* • §170.207(a)(1) - The code set specified at 45 CFR 162.1002(a)(1) for the indicated conditions. • §170.207(a)(2) - IHTSDO SNOMED CT,® July 2009 Version.
	§495.6(d)(4)(i) Generate and transmit permissible prescriptions electronically (eRx). *[75 FR 44337-38]*	§495.6(d)(4)(ii) More than 40% of all permissible prescriptions written by the EP are transmitted electronically using certified EHR technology. *§495.6(d)(4)(iii) - Exclusion: Any EP who writes fewer than 100 prescriptions during the EHR reporting period.*	§170.304(b) Electronic prescribing. Enable a user to electronically generate and transmit prescriptions and prescription-related information in accordance with: (1) The standard specified in §170.205(b)(1) or §170.205(b)(2); and (2) The standard specified in §170.207(d). *[75 FR 44625-27]*	*Electronic prescribing.* • §170.205(b)(1) - NCPDP SCRIPT Version 8.1. • §170.205(b)(2) - NCPDP SCRIPT Version 10.6. *Medications.* • §170.207(d) - Any source vocabulary that is included in RxNorm, a standardized nomenclature for clinical drugs produced by the United States National Library of Medicine.
	§495.6(d)(5)(i) / §495.6(f)(4)(i)	§495.6(d)(5)(ii) / §495.6(f)(4)(ii)	§170.302(d)	

National Institute of Standards and Technology
U.S. Department of Commerce

http://healthit.hhs.gov/media/MU/n508/MU_SCC_CombinedGrid.pdf

From Recommendation to Certified Products



MU Recommendations from ARRA
HIT Policy and Standards Committees

CMS Final Rule – Meaningful Use Objectives and Measures

ONC Final Rule – Certification Criteria and Standards

Approved Test Procedures

ATCB Test Scripts

ATCB Testing of EHRs

ONC Certified Products List

Based on the requirements in the ONC Final Rule, NIST published 42 test procedures which are in use by the authorized testing & certification bodies to test and certify EHR products for the Meaningful Use Program

Accredited Testing and Certification Bodies (ATCBs)

Certification Commission for Health Information Technology Complete EHR and EHR Modules.
Drummond Group, Inc. Complete EHR and EHR Modules.
InfoGard Laboratories, Inc. –Complete EHR and EHR Modules.
ICSA Labs - Complete EHR and EHR Modules.
SLI Global Solutions Complete EHR and EHR Modules.
Surescripts LLC -
EHR Modules: E-Prescribing, Privacy and Security.

http://onc-chpl.force.com/ehrcert

Approved Test Procedures Version 1.1

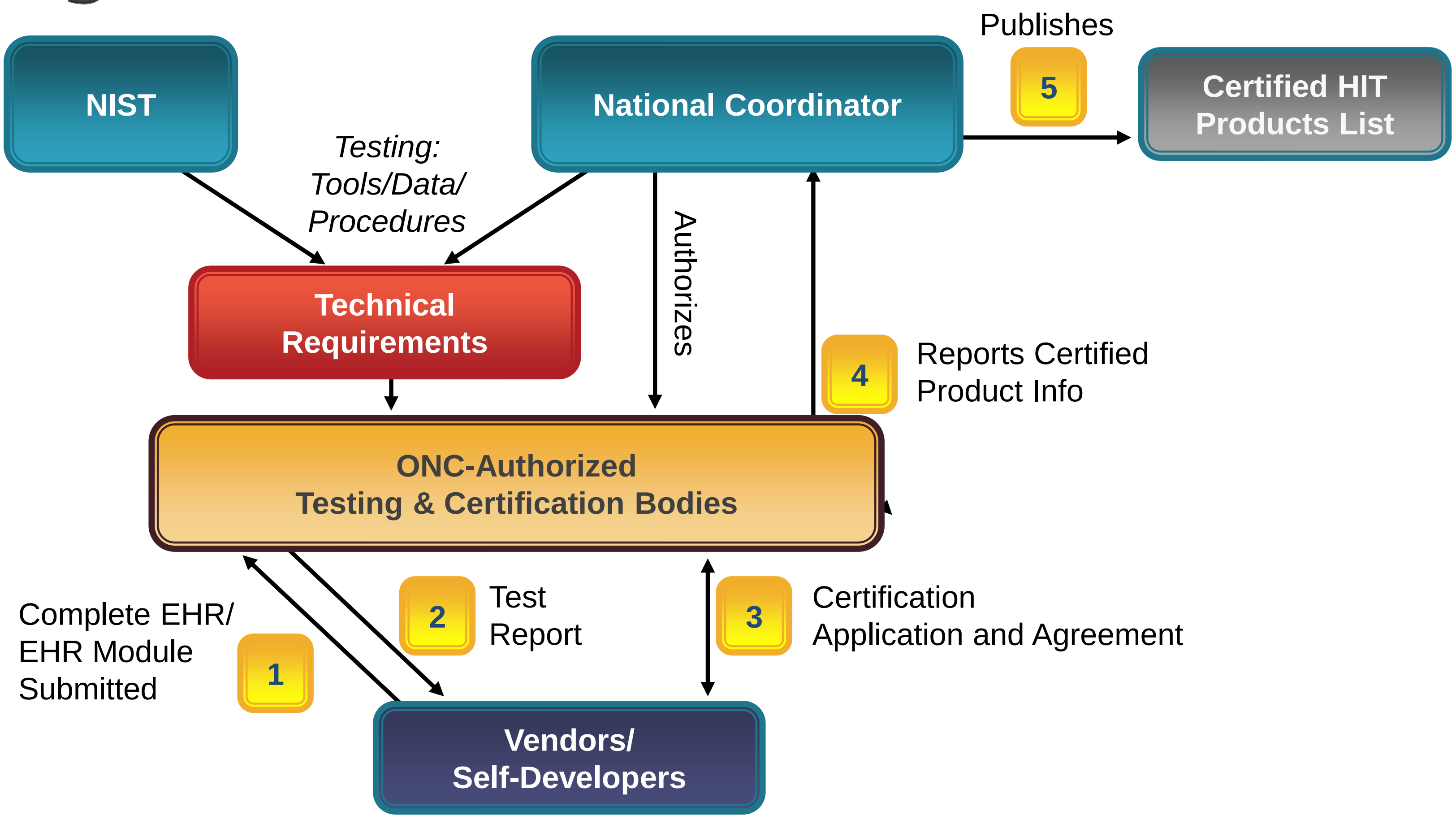
302: All environments
304: Ambulatory
306: In-patient

- §170.302.a Drug-drug, drug allergy, formulary checks
- §170.302.b Drug formulary checks
- §170.302.c Maintain up-to-date problem list *
- §170.302.d Maintain Active Medication List *
- §170.302.e Maintain Active Medication Allergy List
- §170.302.f.1 Vital Signs *
- §170.302.f.2 Body Mass Index
- §170.302.f.3 Growth Charts
- §170.302.g Smoking Status
- §170.302.h Incorporate Lab Test Results *
- §170.302.i Generate Patient Lists
- §170.302.j Medication Reconciliation
- §170.302.k Submission to Immunization Registries *
- §170.302.l Public Health Surveillance (v1.2)
- §170.302.m Education Resources *
- §170.302.n Automate Measure Calculations
- §170.302.o Access Control
- §170.302.p Emergency Access
- §170.302.q Automatic Log-off
- §170.302.r Audit Log
- §170.302.s Integrity
- §170.302.t Authentication
- §170.302.u General Encryption
- §170.302.v Encryption when exchanging electronic health information *
- §170.302.w Accounting of Disclosures
- §170.304.a Computerized Provider Order Entry *
- §170.304.b Electronic Prescribing *
- §170.304.c Record Demographics
- §170.304.d Generate Patient Reminder List
- §170.304.e Clinical Decision Support
- §170.304.f Electronic Copy of Health Information *
- §170.304.g Timely Access
- §170.304.h Clinical Summaries *
- §170.304.i Exchange Clinical Information and Patient Summary Record *
- §170.304.j Calculate & Submit Quality Measures
- §170.306.a Computerized Provider Order Entry
- §170.306.b Record Demographics
- §170.306.c Clinical Decision Support
- §170.306.d.1 Electronic Copy of Health Information *
- §170.306.d.2 Electronic Copy of Health Information
- §170.306.e Electronic Copy of Discharge Information
- §170.306.f Exchange Clinical Information and Patient Summary Record *
- §170.306.g Reportable Lab Results *
- §170.306.h Advance Directives
- §170.306.i Calculate & Submit Quality Measures

*Errata also posted

http://healthcare.nist.gov/use_testing/effective_requirements.html

HHS EHR Temporary Certification Program


NIST
National Coordinator
Publishes
5
Certified HIT Products List
Testing: Tools/Data/ Procedures
Technical Requirements
Authorizes
4
Reports Certified Product Info
ONC-Authorized Testing & Certification Bodies
Complete EHR/ EHR Module Submitted
1
2
Test Report
3
Certification Application and Agreement
Vendors/ Self-Developers

Guiding Principles in the Development of the Test Method (and testing too!)

- 45 CFR Part170 Subpart C is Normative
  - Informative section of FR is not normative
- Constraining the test procedures to the functional and interoperable requirements as stated in the FR
- Describing what needs to be tested and how to perform the testing; not specifying how the Vendor's system should perform a particular function
- Every level of test method is traceable to the criteria
- Do not create new implicit (or explicit) requirements

- No explicit requirements for safety or s/w correctness – focus on functionality

Informative Text Example

Exchange Clinical Information & Summary:

The test procedure is organized into two sections:

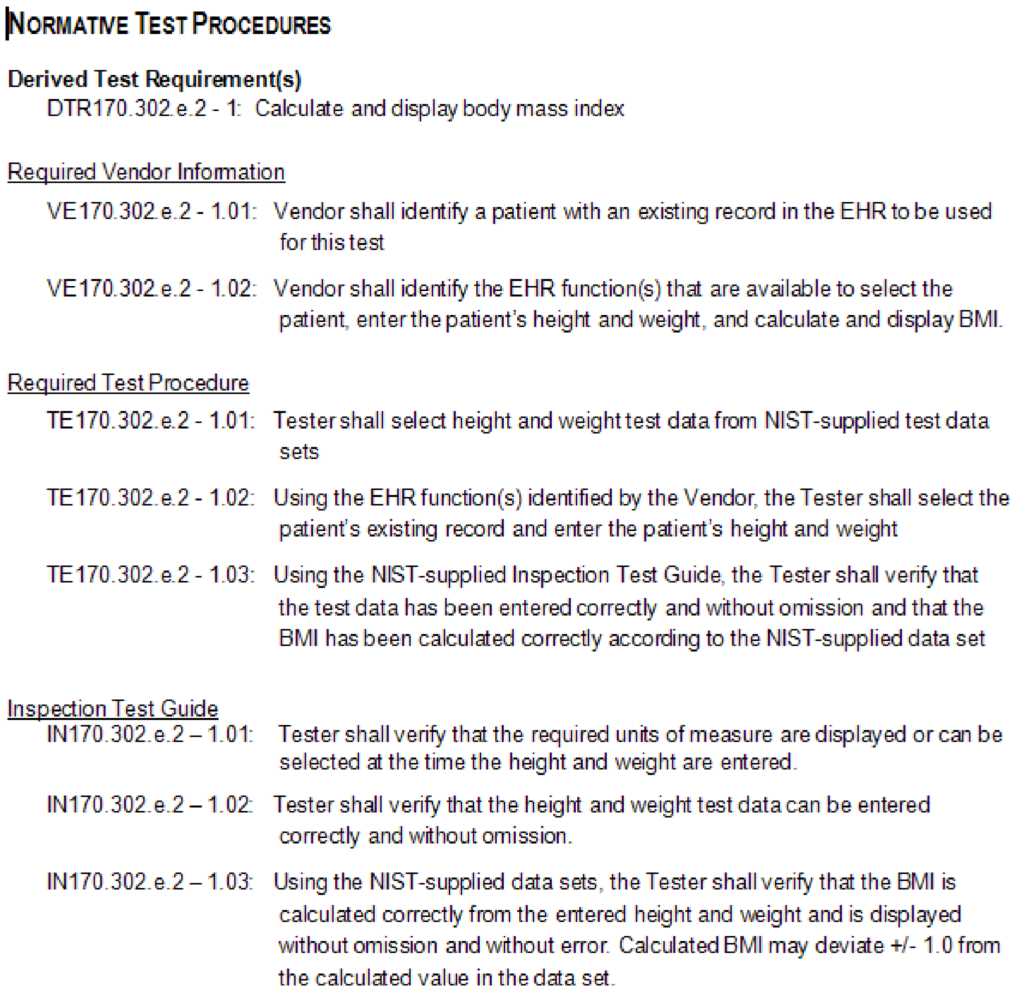
- Receive and Display. evaluates the capability to receive and display (render) a patient summary record in the EHR when received in HL7 CCD format and when received in ASTM CCR format.
  - The patient summary record includes diagnostic test results, problem list, medication list, medication allergy list, immunizations, and procedures. Included in the test procedure is an evaluation of the capability of the EHR to display (render) structured data and vocabulary coded values in human-readable form
- Transmit –evaluates the capability to transmit a patient summary record from the EHR in either HL7 CCD or ASTM CCR format as selected by the Vendor.
  - The patient summary record includes diagnostic test results, problem list, medication list, medication allergy list, immunizations, and procedures. Included in the test procedure is an evaluation of the capability to communicate vocabulary coded values as defined by the referenced standards

A Walk Through the Test Procedures

- Informative section describing
  - Certification criteria as published in 45 CFR Part 170 Subpart C of the Final Rule in the Federal Register on July 13, 2010
  - Informative description of how the test procedure is organized and conducted
  - Standards referenced in the certification criteria
- Normative Test Procedure
  - Describes the required vendor information and test requirements for validating conformance to the criteria and standards
- Example Test Data
  - Provides examples of the test data to be used during the test procedure. The test data sets will be expanded as the test method matures.
- Conformance Test Tools
  - Provides a description and links to the associated conformance test tools, if applicable, to evaluate conformance to the referenced standards.

The normative test procedure provides information for validating conformance to the criteria and standards

- Each subsection provides additional information on:
  - Required vendor information
  - Required test procedures
  - Inspection test guide
- Traceability is provided in each subsection through a unique numbering sequence



NORMATIVE TEST PROCEDURES

Derived Test Requirement(s)

DTR170.302.e.2 - 1: Calculate and display body mass index

Required Vendor Information

VE170.302.e.2 - 1.01: Vendor shall identify a patient with an existing record in the EHR to be used for this test

VE170.302.e.2 - 1.02: Vendor shall identify the EHR function(s) that are available to select the patient, enter the patient's height and weight, and calculate and display BMI.

Required Test Procedure

TE170.302.e.2 - 1.01: Tester shall select height and weight test data from NIST-supplied test data sets

TE170.302.e.2 - 1.02: Using the EHR function(s) identified by the Vendor, the Tester shall select the patient's existing record and enter the patient's height and weight

TE170.302.e.2 - 1.03: Using the NIST-supplied Inspection Test Guide, the Tester shall verify that the test data has been entered correctly and without omission and that the BMI has been calculated correctly according to the NIST-supplied data set

Inspection Test Guide

IN170.302.e.2 – 1.01: Tester shall verify that the required units of measure are displayed or can be selected at the time the height and weight are entered.

IN170.302.e.2 – 1.02: Tester shall verify that the height and weight test data can be entered correctly and without omission.

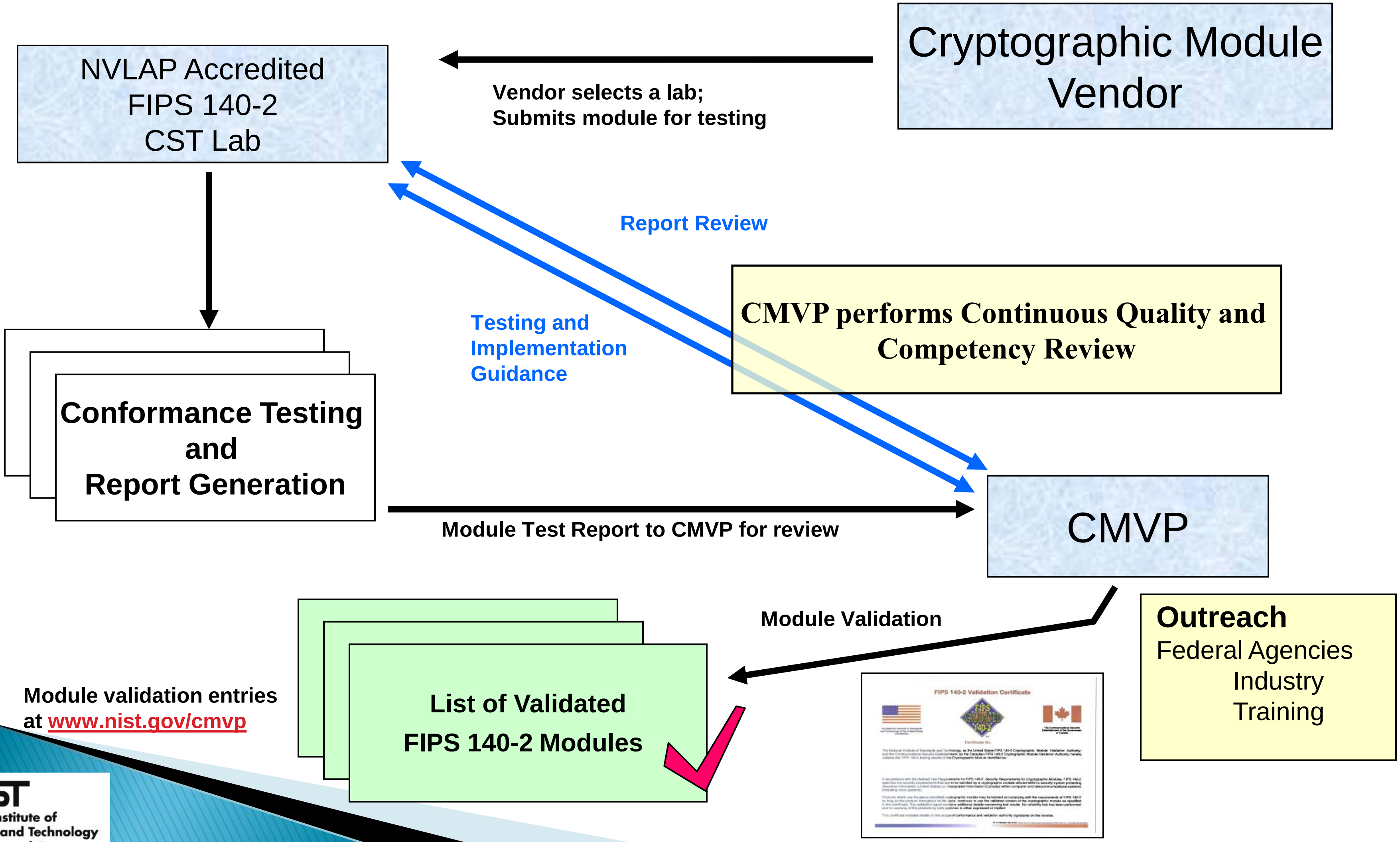
IN170.302.e.2 – 1.03: Using the NIST-supplied data sets, the Tester shall verify that the BMI is calculated correctly from the entered height and weight and is displayed without omission and without error. Calculated BMI may deviate +/- 1.0 from the calculated value in the data set.

NIST Cryptographic Module Validation Program

- Program validates cryptographic modules to FIPS 140-2 (update to FIPS 140-1) *Security Requirements for Cryptographic Modules*
- Joint effort – NIST and Communications Security Establishment Canada (CSEC)
- h/w & s/w modules; four levels of increasing requirements (breadth and depth)
- Derived Test Requirements contain tests
- Implementaion Guidance – incorporate lessons-learned; new technologies
- Mature – established in July 1995
- 1500+ Validations issued!

Cryptographic Module Validation Program – Model

Test and Validation



Cryptographic Module Vendor

Vendor selects a lab;
Submits module for testing

NVLAP Accredited
FIPS 140-2
CST Lab

Report Review

Testing and Implementation Guidance

CMVP performs Continuous Quality and Competency Review

Conformance Testing and Report Generation

Module Test Report to CMVP for review

CMVP

Module Validation

Outreach
Federal Agencies
Industry
Training

List of Validated FIPS 140-2 Modules

Module validation entries at www.nist.gov/cmvp

FIPS 140-2 Validation Certificate

Common Issues

- Givens:
  - Requirements in the form of functionality
  - Requirements often don't include software quality, safety, correctness
  - Regulatory timeframes present challenges
  - Audience is not testing/certification aware
- The resources for re-test/re-cert grow to become the larger expense.
  - Planning for this in operations is critical
    - After initial market saturation; re-test/re-cert is focus
  - CMVP – experiences this (1500 validations issued)
  - HHS EHR Cert Program – still in 'initial test' in the market

Moving Forward

To the SCC participants:

#1 How can the two approaches come together a priori (regulatory timeframe) for markets w/large numbers of vendors & products to certify? (e.g., HIT Certs = ~580 in 7 months)

#2 Can s/w cert techniques be used to solve the re-test problem now?

#3 Long-term strategy: Challenge to educate decision-makers that s/w process certification will give them success (functionality) for the cost

NIST National Institute of Standards and Technology U.S. Department of Commerce