§170.315(a)(2) Computerized provider order entry (CPOE) – laboratory

2015 Edition CCGs

Version 1.1 Updated on 12-10-2015

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	10-22-2015
1.1	Revised to include clarification about developer discretion for implementing the optional provision.	12-10-2015

Regulation Text

Regulation Text

§170.315 (a)(2) *Computerized provider order entry—laboratory—*

(i) Enable a user to record, change, and access laboratory orders.

(ii) *Optional.* Include a "reason for order" field.

Standard(s) Referenced

None

Certification Companion Guide: Computerized provider order entry (CPOE) – laboratory

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
Unchanged	Yes	Included	Yes

Certification Requirements

Privacy and Security: This certification criterion was adopted at § 170.315(a)(2). As a result, an ONC-ACB must ensure that a product presented for certification to a § 170.315(a) "paragraph (a)" 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 presented 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) "VDT" and (e)(2) "secure messaging," which are explicitly stated.

Table for Privacy and Security

- 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))
  - Amendments (§ 170.315(d)(4))
  - Automatic access time-out (§ 170.315(d)(5))
  - Emergency access (§ 170.315(d)(6))
  - End-user device encryption (§ 170.315(d)(7))
- If choosing Approach 2:
  - For each applicable P&S certification criterion not certified for approach 1, the health IT developer may certify for the criterion using system documentation which provides a clear description of how the external services necessary to meet the P&S criteria would be deployed and used. Please see the 2015 Edition final rule correction notice at 80 FR 76870 for additional clarification.

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

- Safety-enhanced design (§ 170.315(g)(3)) must be explicitly demonstrated for this criterion.
- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- 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.

Table for Design and Performance

- Safety-enhanced design (§ 170.315(g)(3))
- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- There is no standard required for this certification criterion.
- To meet the 2015 Edition Base EHR definition, providers must possess technology that has been certified to at least one of the following: § 170.315(a)(1) Computerized provider order entry (CPOE) – medications, § 170.315(a)(2) Computerized provider order entry (CPOE) – laboratory, or § 170.315(a)(3) Computerized provider order entry (CPOE) – diagnostic imaging.

Paragraph (a)(2)(i)

Technical outcome – The health IT permits a user to record, change, and access laboratory orders.

Clarifications:

- No standard is required for demonstrating the ability to allow a user to record, change, and access laboratory orders.
- This provision does not focus on the transmission of laboratory orders, only on the ability of a user to record, change, and access the laboratory order. [see also 77 FR 54248] and [see also 75 FR 44624]

Paragraph (a)(2)(ii) *Optional*

Technical outcome – The health IT allows for the user to include a "reason for order."

Clarifications:

- It is not mandatory to allow a user to include a "reason for order" field, however it is optional. The developer has the discretion to determine how to implement this optional provision (e.g., free text field or drop-down menu of pre-determined entries).

Content last reviewed on September 21, 2018