Drug-drug, drug-allergy interaction checks for CPOE

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (a)(4) *Drug-drug, drug-allergy interaction checks for CPOE—*

1. *Interventions.* Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.
2. *Adjustments.*
    1. Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.
    2. Limit the ability to adjust severity levels in at least one of these two ways:
        1. To a specific set of identified users.
        2. As a system administrative function.

Standard(s) Referenced

None

Certification Dependencies

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.
- 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, the QMS' need to be 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.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(a)(4). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(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) “View, download, and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging,” which are explicitly stated.
- Health IT presented for certification to this criterion (Drug-drug, drug-allergy interaction checks for CPOE) would not have to demonstrate the capabilities required by the Amendments certification criterion (§ 170.315(d)(4)), unless the health IT is presented for certification to another criterion that requires certification to the Amendments criterion under the privacy and security certification framework.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

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

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 which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25710 for additional clarification.

Revision History

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

Regulation Text

Regulation Text

§ 170.315 (a)(4) *Drug-drug, drug-allergy interaction checks for CPOE—*

1. *Interventions.* Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.
2. *Adjustments.*
    1. Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.
    2. Limit the ability to adjust severity levels in at least one of these two ways:
        1. To a specific set of identified users.
        2. As a system administrative function.

Standard(s) Referenced

None

Certification Dependencies

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.
- 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, the QMS' need to be 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.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(a)(4). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(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) “View, download, and transmit to 3rd party (VDT)” and (e)(2) “Secure messaging,” which are explicitly stated.
- Health IT presented for certification to this criterion (Drug-drug, drug-allergy interaction checks for CPOE) would not have to demonstrate the capabilities required by the Amendments certification criterion (§ 170.315(d)(4)), unless the health IT is presented for certification to another criterion that requires certification to the Amendments criterion under the privacy and security certification framework.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

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))
  - 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 which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25710 for additional clarification.

Revision History

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

Testing components

Attestation: As of September 21, 2017, the testing approach for this criterion is satisfied by attestation.

The archived version of the Test Procedure is attached below for reference.

System Under Test	ONC-ACB Verification
The health IT developer will attest directly to the ONC-ACB to conformance with the §170.315(a)(4) *Drug-drug, drug-allergy interaction checks for CPOE* requirements.	The ONC-ACB verifies the health IT developer attests conformance to the §170.315(a)(4) *Drug-drug, drug-allergy interaction checks for CPOE* requirements.

Archived Version:
§170.315(a)(4) Test Procedure
Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (a)(4) *Drug-drug, drug-allergy interaction checks for CPOE—*

1. *Interventions.* Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.
2. *Adjustments.*
    1. Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.
    2. Limit the ability to adjust severity levels in at least one of these two ways:
        1. To a specific set of identified users.
        2. As a system administrative function.

Standard(s) Referenced

None

Certification Dependencies

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.
- 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, the QMS' need to be 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.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(a)(4). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(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) "View, download, and transmit to 3rd party (VDT)" and (e)(2) "Secure messaging," which are explicitly stated.
- Health IT presented for certification to this criterion (Drug-drug, drug-allergy interaction checks for CPOE) would not have to demonstrate the capabilities required by the Amendments certification criterion (§ 170.315(d)(4)), unless the health IT is presented for certification to another criterion that requires certification to the Amendments criterion under the privacy and security certification framework.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

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))
  - 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 which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25710 for additional clarification.

Revision History

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

Regulation Text

Regulation Text

§ 170.315 (a)(4) *Drug-drug, drug-allergy interaction checks for CPOE—*

1. *Interventions.* Before a medication order is completed and acted upon during computerized provider order entry (CPOE), interventions must automatically indicate to a user drug-drug and drug-allergy contraindications based on a patient's medication list and medication allergy list.
2. *Adjustments.*
    1. Enable the severity level of interventions provided for drug-drug interaction checks to be adjusted.
    2. Limit the ability to adjust severity levels in at least one of these two ways:
        1. To a specific set of identified users.
        2. As a system administrative function.

Standard(s) Referenced

None

Certification Dependencies

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.
- 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, the QMS' need to be 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.

Privacy & Security Requirements

This certification criterion was adopted at § 170.315(a)(4). As a result, an ONC Authorized Certification Body (ONC-ACB) must ensure that a product presented for certification to a § 170.315(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) "View, download, and transmit to 3rd party (VDT)" and (e)(2) "Secure messaging," which are explicitly stated.
- Health IT presented for certification to this criterion (Drug-drug, drug-allergy interaction checks for CPOE) would not have to demonstrate the capabilities required by the Amendments certification criterion (§ 170.315(d)(4)), unless the health IT is presented for certification to another criterion that requires certification to the Amendments criterion under the privacy and security certification framework.
- § 170.315(d)(2)(i)(C) is not required if the scope of the Health IT Module does not have end-user device encryption features.

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))
  - 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 which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces the Health IT Module to access external services necessary to meet the requirements of the privacy and security certification criterion. Please see the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program* Final Rule at 85 FR 25710 for additional clarification.

Revision History

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

Certification Companion Guide: Drug-drug, drug-allergy interaction checks for CPOE

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product certification. The CCG is not a substitute for the requirements outlined in regulation and related ONC final rules. It extracts key portions of ONC final rules' preambles and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the Certification Regulations page for links to all ONC final rules or consult other regulatory references as noted. The CCG is for public use and should not be sold or redistributed.

The below table outlines whether this criterion has additional Maintenance of Certification dependencies, update requirements and/or eligibility for standards updates via SVAP. Review the Certification Dependencies and Required Update Deadline drop-downs above if this table indicates "yes" for any field.

Base EHR Definition	Real World Testing	Insights Condition	SVAP	Requires Updates
Not Included	No	No	No	No

Certification Requirements

Technical Explanations and Clarifications

Applies to entire criterion

Clarifications:

- There is no standard required for this certification criterion.
- The scope of this criterion is on the health IT system's ability to perform drug-drug, drug-allergy interaction checks during CPOE. Certification to this criterion does not require the system to perform drug-drug, drug-allergy interaction checks in other cases, such as when medications are reviewed or medication/medication allergy lists are updated. [see also 75 FR 44602; 77 FR 54206; 80 FR 62618]
- No standards are required for this criterion, but checks are only expected to be performed based upon structured data. [see also 75 FR 44602]
- For testing and certification purposes, drug-allergy contraindications include adverse reaction contraindications. [see also 77 FR 54208]
- This criterion is separate and distinct from the § 170.315(a)(9) "Clinical decision support" criterion. [see also 77 FR 54208]
- How the interventions are automatically indicated to a user is at the discretion of the developer and they have the flexibility to implement this functionality based on their customer preferences and in line with their user-centered design requirements.

Clarifications:

- There is no standard required for this certification criterion.
- The scope of this criterion is on the health IT system's ability to perform drug-drug, drug-allergy interaction checks during CPOE. Certification to this criterion does not require the system to perform drug-drug, drug-allergy interaction checks in other cases, such as when medications are reviewed or medication/medication allergy lists are updated. [see also 75 FR 44602; 77 FR 54206; 80 FR 62618]
- No standards are required for this criterion, but checks are only expected to be performed based upon structured data. [see also 75 FR 44602]
- For testing and certification purposes, drug-allergy contraindications include adverse reaction contraindications. [see also 77 FR 54208]
- This criterion is separate and distinct from the § 170.315(a)(9) "Clinical decision support" criterion. [see also 77 FR 54208]
- How the interventions are automatically indicated to a user is at the discretion of the developer and they have the flexibility to implement this functionality based on their customer preferences and in line with their user-centered design requirements.

Paragraph (a)(4)(i) Interventions

Technical outcome – Interventions should automatically occur during CPOE and before the medication order is completed and acted on.

Clarifications:

> A Health IT Module is only expected to perform drug-drug, drug-allergy interaction checks based on medication and medication allergy information included in the system as structured data. The Health IT Module is not expected to be capable of reading or accessing information in non-structured formats (e.g., scanned documents, images) for this provision. [see also 75 FR 44602]

Technical outcome – Interventions should automatically occur during CPOE and before the medication order is completed and acted on.

Clarifications:

> A Health IT Module is only expected to perform drug-drug, drug-allergy interaction checks based on medication and medication allergy information included in the system as structured data. The Health IT Module is not expected to be capable of reading or accessing information in non-structured formats (e.g., scanned documents, images) for this provision. [see also 75 FR 44602]

Paragraph (a)(4)(ii)(A) Adjustments – Enable severity level

Technical outcome – The health IT allows a user to adjust the level for drug-drug interaction interventions provided.

Clarifications:

- This functionality does not need to be provided to every user; testing and certification will ensure that the functionality exists for authorized users. [see also 77 FR 54208]
- This functionality only adjusts what may display to an end user. It does not change the severity level/clinical significance of an interaction or contraindication but allows authorized users to tailor the interventions the users receive.

Technical outcome – The health IT allows a user to adjust the level for drug-drug interaction interventions provided.

Clarifications:

- This functionality does not need to be provided to every user; testing and certification will ensure that the functionality exists for authorized users. [see also 77 FR 54208]
- This functionality only adjusts what may display to an end user. It does not change the severity level/clinical significance of an interaction or contraindication but allows authorized users to tailor the interventions the users receive.

Paragraph (a)(4)(ii)(B) Adjustments – limit to identified set of users

Technical outcome – The ability to adjust drug-drug, drug-allergy interactions should be able to be limited to an identified set of users.

Clarifications:

> “Identified set of users’’ means that the technology must enable a provider to assign only certain users (e.g., specific providers, system administrator) with the ability to adjust severity levels for drug-drug, drug-allergy interaction interventions. [see also 77 FR 54208]

Technical outcome – The ability to adjust drug-drug, drug-allergy interactions should be able to be limited to an identified set of users.

Clarifications:

> “Identified set of users’’ means that the technology must enable a provider to assign only certain users (e.g., specific providers, system administrator) with the ability to adjust severity levels for drug-drug, drug-allergy interaction interventions. [see also 77 FR 54208]