Emergency access | HealthIT.gov

§170.315(d)(6) Emergency access

- Certification Companion Guide (CCG)
- Conformance Method

Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(6) *Emergency access*—

Permit an identified set of users to access electronic health information during an emergency.

Standard(s) Referenced

None

Certification Dependencies

Design and performance: Quality management system (§ 170.315(g)(4)) and accessibility-centered design (§ 170.315(g)(5)) must be certified as part of the overall scope of the certificate issued to the product.

- 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.

Revision History

Version #	Description of Change	Version Date

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

Regulation Text

Regulation Text

§ 170.315 (d)(6) *Emergency access*—

Permit an identified set of users to access electronic health information during an emergency.

Standard(s) Referenced

None

Certification Dependencies

Design and performance: Quality management system (§ 170.315(g)(4)) and accessibility-centered design (§ 170.315(g)(5)) must be certified as part of the overall scope of the certificate issued to the product.

- 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.

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(d)(6) *Emergency access* requirements.	The ONC-ACB verifies the health IT developer attests conformance with the §170.315(d)(6) *Emergency access* requirements.

Archived Version:
§170.315(d)(6) Test Procedure
Updated on 03-11-2024

Regulation Text

Regulation Text

§ 170.315 (d)(6) *Emergency access*—

Permit an identified set of users to access electronic health information during an emergency.

Standard(s) Referenced

None

Certification Dependencies

Design and performance: Quality management system (§ 170.315(g)(4)) and accessibility-centered design (§ 170.315(g)(5)) must be certified as part of the overall scope of the certificate issued to the product.

- 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.

Revision History

Version #	Description of Change	Version Date

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

Regulation Text

Regulation Text

§ 170.315 (d)(6) *Emergency access*—

Permit an identified set of users to access electronic health information during an emergency.

Standard(s) Referenced

None

Certification Dependencies

Design and performance: Quality management system (§ 170.315(g)(4)) and accessibility-centered design (§ 170.315(g)(5)) must be certified as part of the overall scope of the certificate issued to the product.

- 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.

Revision History

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

Certification Companion Guide: Emergency access

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

Technical outcome – The health IT must be able to grant access to an identified set of users during an emergency.

Clarifications:

- There is no standard associated with this criterion.
- The criterion is not intended to specify what constitutes an emergency or who would be authorized to access electronic health information in an emergency. Those determinations should be made with applicable state and federal laws, organizational policies and procedures, and the relevant standard of care. Likewise, an “emergency” is not limited to clinical or life threatening emergencies but could include other scenarios such as those related to normal patient care when timely access to electronic health information becomes critical. [see also 75 FR 44617]
- ONC believes this criterion is consistent with the HIPAA Security Final Rule (68 FR 8355), which states “We believe that emergency access is a necessary part of access controls and, therefore, is properly a required implementation specification of the “Access controls” standard. Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.” [see also 75 FR 44617]

- Emergency access is intended to cover a broad range of scenarios, including life threatening emergencies related to the patient as well as normal patient care where timely access to electronic health information becomes critical. [see also 75 FR 44617]
- Emergency access is part of a Health IT' Module's general access control and should be established before the emergency, potentially as a “pre-set” function. [see also 75 FR 44617] The goal of the capability is to ensure that there is a way for identified users to have access (e.g., by elevating their access privileges) in an emergency to gain or maintain access to patient health information, which should be an auditable event. [see also 80 FR 62655] In sum, the "emergency access" functionality should be demonstrated based on the access rules already built into the Health IT Module.

Technical outcome – The health IT must be able to grant access to an identified set of users during an emergency.

Clarifications:

- There is no standard associated with this criterion.
- The criterion is not intended to specify what constitutes an emergency or who would be authorized to access electronic health information in an emergency. Those determinations should be made with applicable state and federal laws, organizational policies and procedures, and the relevant standard of care. Likewise, an “emergency” is not limited to clinical or life threatening emergencies but could include other scenarios such as those related to normal patient care when timely access to electronic health information becomes critical. [see also 75 FR 44617]
- ONC believes this criterion is consistent with the HIPAA Security Final Rule (68 FR 8355), which states “We believe that emergency access is a necessary part of access controls and, therefore, is properly a required implementation specification of the “Access controls” standard. Access controls will still be necessary under emergency conditions, although they may be very different from those used in normal operational circumstances. For example, in a situation when normal environmental systems, including electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster, procedures should be established beforehand to provide guidance on possible ways to gain access to needed electronic protected health information.” [see also 75 FR 44617]
- Emergency access is intended to cover a broad range of scenarios, including life threatening emergencies related to the patient as well as normal patient care where timely access to electronic health information becomes critical. [see also 75 FR 44617]
- Emergency access is part of a Health IT' Module's general access control and should be established before the emergency, potentially as a “pre-set” function. [see also 75 FR 44617] The goal of the capability is to ensure that there is a way for identified users to have access (e.g., by elevating their access privileges) in an emergency to gain or maintain access to patient health information, which should be an auditable event. [see also 80 FR 62655] In sum, the "emergency access" functionality should be demonstrated based on the access rules already built into the Health IT Module.

Form Approved OMB# 0990-0379 Exp. Date 9/30/2025

Content last reviewed on March 11, 2024