

# 2015 Edition Certification Companion Guide

## Emergency Access - 45 CFR 170.315(d)(6)

### [Final Rule Preamble – Test Procedure](#)

Version 1.2 – Last Updated 7/20/2016

| New/Revised/Unchanged Compared to 2014 Edition | Gap Certification Eligible | Base EHR Definition | Certified EHR Technology Definition | Associated EHR Incentive Program Objective(s) |
|--|----------------------------|---------------------|-------------------------------------|---|
| Unchanged                                      | Yes                        | No                  | Not Included                        | N/A   |

### Certification Requirements

[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.

- 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.

### Regulation Text

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

| Criterion Subparagraph      | Technical Explanations and Clarifications   | Standard(s) Referenced |
|-----------------------------|---|------------------------|
| Applies to entire criterion | <ul style="list-style-type: none"> <li>• Technical outcome – The health IT must be able to grant access to an identified set of users during an emergency.</li> </ul> <p><b>Clarifications:</b></p> <ul style="list-style-type: none"> <li>• There is no standard associated with this criterion.</li> <li>• 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 <a href="#">75 FR 44617</a>]</li> </ul> | N/A                    |

| Criterion Subparagraph                 | Technical Explanations and Clarifications  | Standard(s) Referenced |
|--|--|------------------------|
| Applies to entire criterion, continued | <ul style="list-style-type: none"> <li>• We believe 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 <a href="#">75 FR 44617</a>]</li> <li>• Although this criterion is gap certification eligible, note that emergency access capabilities are expected to be performed electronically as required for certification to the 2015 Edition unless specified. We recommend ATLS and ONC-ACBs ensure that systems certified to the 2014 Edition emergency access certification criterion provide this capability electronically if presenting for gap certification. [see also <a href="#">80 FR 62610</a>]</li> <li>• 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 <a href="#">75 FR 44617</a>].</li> <li>• 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 <a href="#">75 FR 44617</a>] 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 <a href="#">80 FR 62655</a>] In sum, the "emergency access" functionality should be demonstrated based on the access rules already built into the Health IT Module.</li> </ul> | N/A                    |

**Note:** 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.

**Version History**

| Version # | Change(s) Summary   | Date Made    |
|-----------|---|--------------|
| 1.0       | Initial Publication   | Oct 22, 2015 |
| 1.1       | Added clarification that emergency access capabilities must be provided electronically. | Dec 18, 2015 |

| Version # | Change(s) Summary   | Date Made    |
|-----------|---|--------------|
| 1.2       | Clarification added to explain the scope of emergency access. Clarification and guidance also provided for demonstrating compliance with the criterion. | Jul 20, 2016 |