We propose to adopt a 2015 Edition "amendments" certification criterion that is unchanged in comparison to the 2014 Edition "amendments" criterion (§ 170.314(d)(4)). We note that this certification criterion only partially addresses the amendment of protected health information (PHI) requirements of 45 CFR 164.526.

- Automatic Access Time-Out

| **2015 Edition Health IT Certification Criterion** |
| --- |
| § 170.315(d)(5) (Automatic access time-out) |

We propose to adopt a 2015 Edition "automatic access time-out" certification criterion that is unchanged (for the purposes of gap certification) in comparison to the 2014 Edition "automatic log-off" criterion (§ 170.314(d)(5)). The 2014 Edition "automatic log-off" criterion requires a Health IT Module to "prevent a user from gaining further access to an electronic session after a predetermined time of inactivity." In June 2014, the Privacy and Security Workgroup (PSWG) of the HITSC assessed the automatic log-off criterion.[140] While the 2014 Edition criterion refers to "sessions," the PSWG noted the need to recognize that many systems are not session-based. Instead, systems may be stateless, clientless, and/or run on any device. The PSWG further noted that the risk that this criterion addresses is the potential that protected health information could be disclosed through an unattended device. The HITSC recommended that this certification criterion should not be overly prescriptive so as to inhibit system architecture flexibility.

To clarify this intent and eliminate the reference to "session," the PSWG suggested to the HITSC that this criterion by refined to state "automatically block access to protected health information after a predetermined period of inactivity through appropriate means until the

[140] http://www.healthit.gov/facas/sites/faca/files/HITSC_PSWG_2015NPRM_Update_2014-06-17.pdf

original user re-authenticates or another authorized user authenticates." We agree in substance with the PSWG work and HITSC recommendations. Accordingly, we propose a 2015 Edition "automatic access time-out" certification criterion that reflects the HITSC recommendations and the work of the PSWG. Specifically, the criterion would require a Health IT Module to demonstrate that it can automatically stop user access to health information after a predetermined period of inactivity and require user authentication in order to resume or regain the access that was stopped. We note, however, that we do not believe this would have any impact on testing and certification as compared to testing and certification to the 2014 Edition "automatic log-off" criterion (i.e., the 2015 "automatic access time-out" criterion would be eligible for gap certification). We welcome comments on this assessment.

- Emergency Access

| **2015 Edition Health IT Certification Criterion** |
| --- |
| § 170.315(d)(6) (Emergency access) |

We propose to adopt a 2015 Edition "emergency access" certification criterion that is unchanged in comparison to the 2014 Edition "emergency access" criterion (§ 170.314(d)(6)).

- End-User Device Encryption

| **2015 Edition Health IT Certification Criterion** |
| --- |
| § 170.315(d)(7) (End-user device encryption) |

We propose to adopt a 2015 Edition "end-user device encryption" certification criterion that is unchanged (for the purposes of gap certification) in comparison to the 2014 Edition "end-user device encryption" criterion (§ 170.314(d)(7)). We propose to require certification to this criterion consistent with the most recent version of Annex A: Approved Security Functions (Draft, October 8, 2014) for Federal Information Processing Standards (FIPS) Publication 140-

2.[141] The purpose of this document is to provide a list of the approved security functions applicable to FIPS PUB 140-2. To maintain and update our certification requirements to the most recent NIST-approved security functions, we propose to move to the updated version of Annex A (Draft, October 8, 2014). We proposed to adopted this updated version of Annex A at § 170.210(a)(3). We note, however, that we do not believe that this would have any impact on testing and certification as compared to testing and certification to the 2014 Edition "end-user device encryption" criterion (i.e., the 2015 "end-user device encryption" criterion would be eligible for gap certification). We welcome comments on this assessment.

- Integrity

| **2015 Edition Health IT Certification Criterion** |
| --- |
| § 170.315(d)(8) (Integrity) |

We propose to adopt a 2015 Edition "integrity" certification criterion that is unchanged in comparison to the 2014 Edition "integrity" criterion (§ 170.314(d)(8)). However, we propose a change in how a Health IT Module would be tested and certified to this criterion. The 2011 and 2014 editions of this criterion have been available for individual testing and certification. We propose that the 2015 Edition "integrity" criterion would be tested and certified to support the context for which it was adopted – upon receipt of a summary record in order to ensure the integrity of the information exchanged (see § 170.315(d)(8)(ii)). Therefore, we expect that this certification criterion would most frequently be paired with the ToC certification criterion for testing and certification.

[141] http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

In the 2014 Edition propose rule, we sought comment on whether we should leave the standard for the 2014 Edition "integrity" certification criterion as SHA–1[142] or replace it with SHA-2[143], as SHA-2 is a much stronger security requirement. In the 2014 Edition final rule (77 FR 54251), we determined that the SHA–1 standard should serve as a floor and technology could be certified to the 2014 Edition "integrity" certification criterion if it included hashing algorithms with security strengths equal to or greater than SHA–1. We also noted that the Direct Project specification requires that SHA-1 and SHA-256 (one type of SHA–2 hash algorithms) be supported, which still remains the case today.

It is our understanding that many companies, including Microsoft and Google, plan to sunset (deprecate) SHA–1 no later than January 1, 2017.[144] While the SHA–1 standard serves as the baseline standard for certification to the proposed 2015 Edition "integrity" certification criterion and health IT could be certified to a security strength greater than SHA–1 (e.g., SHA–2), we seek comments on if, and when, we should set the baseline for certification to the 2015 Edition "integrity" certification criterion at SHA–2. For example, we could adopt and move to SHA–2 as the baseline certification requirement with the effective date of a subsequent file rule. This would likely be in late 2015 (considering the start of testing and certification), and consistent with the current trajectory of the industry in this area. Alternatively, we could set an effective date within the criterion for when the baseline for certification would shift from SHA–1 to SHA–2 (e.g., beginning 2017).

- Accounting of Disclosures

---

[142] http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[143] http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
[144] http://www.symantec.com/en/au/page.jsp?id=sha2-transition

C. Health IT Module Certification Requirements

1. Privacy and Security

We propose a new approach for privacy and security (P&S) certification to the 2015 Edition. In our past rulemakings, we have discussed and instituted two different policy approaches and sought comment on others for ensuring that health IT and providers have privacy and security capabilities while also trying to minimize the level of regulatory burden imposed on health IT developers. In the 2011 Edition, we included an upfront requirement that required Health IT Modules to meet all P&S certification criteria as a condition of certification unless the health IT developer could demonstrate that certain P&S capabilities were either technically infeasible or inapplicable. In the 2014 Edition, we eliminated the upfront requirement for each Health IT Module to be certified against the P&S criteria in favor of what we thought would better balance the burden potentially posed by our rulemaking. Thus, the P&S criteria were made part of the "2014 Edition Base EHR definition" that all EPs, EHs, and CAHs must meet in order to satisfy the CEHRT definition (meaning each provider needed, post-certification to ultimately have technology certified to the P&S criteria).

On March 23, 2013, the HITSC recommended that we should change our certification policy for P&S. They recommended that each Health IT Module presented for certification should be certified through one or more of the following three paths:

- Demonstrate, through system documentation and certification testing, that the Health IT Module includes functionality that meets at least the "minimal set"[229] of privacy and security certification criterion.

[229] The minimal set includes the following certification criteria: "authentication, access control, and authorization," "auditable events and tamper resistance," "audit report(s)," "amendments," "automatic log-off," "emergency

- Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces that enable it to access external services necessary to conform to the "minimal set" of privacy and security certification criterion.
- Demonstrate through documentation that the privacy and security certification criterion (and the minimal set that the HITSC defined) is inapplicable or would be technically infeasible for the Health IT Module to meet. In support of this path, the HITSC recommended that ONC develop guidance on the documentation required to justify inapplicability or infeasibility.

In response to the HITSC recommendations and stakeholder feedback we sought comment in the Voluntary Edition proposed rule (79 FR 10925-26) on the following four options we believed could be applied to Health IT Module certification for privacy and security: (1) re-adopt the 2011 Edition approach; (2) maintain the 2014 Edition approach; (3) adopt the 2013 HITSC recommendation; or (4) adopt a limited applicability approach – under which ONC would establish a limited set of P&S functionality that every Health IT Module would be required to address in order to be certified.

In response to our request for comments, we received comments generally in support of the 2014 approach (including P&S in the Base EHR definition). While some commenters supported requiring a subset of P&S criteria (option 4), many disagreed on the scope and did not see the value vis-a-vis HIPAA compliance. The HITSC preferred a different option. They recommended that ONC revise each privacy and security criterion to specify the conditions under which it is

---

access," "end-user device encryption," and "integrity." The full recommendation can be found at: http://www.healthit.gov/sites/default/files/pswgtransmittalmemo_032613.pdf.

applicable (similar to how the end-user device encryption criterion currently is written), and allow each criterion to be met using one of the three paths the HITSC recommended in 2013.[230]

During their discussions regarding the Voluntary Edition proposed rule, the HITSC's Privacy and Security Workgroup (PSWG) completed an assessment of which P&S functionality should be required for each proposed certification criterion. The PSWG recognized that the privacy and security criteria are not equally applicable or useful to every criterion in each of the other regulatory functional areas (i.e., clinical, care coordination, clinical quality, patient engagement, public health, utilization, and transmission) because each P&S criterion is designed to address specific risk conditions that may or may not be present within a specific regulatory functional area.

The PSWG model allows for the appropriate safeguards to be in place for each criterion, without overburdening health IT developers by requiring them to include all P&S functionality for each criterion. We believe this serves as a good model, in combination with the 2013 HITSC recommendations, to propose a new, simpler, straight-forward approach to the P&S certification requirements for Health IT Modules that merges many of the recommendations and feedback we have received to date. Under the proposed approach, a health IT developer would know exactly what it needed to do in order to get its Health IT Module certified and a purchaser of a Health IT Module would know exactly what privacy and security functionality against which the Health IT Module had to be tested in order to be certified.

We propose to require that an ONC-ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into each regulatory text "first level

---

[230] http://www.healthit.gov/sites/default/files/pswgtransmittalmemo_032613.pdf

paragraph" category (e.g., § 170.315(a)) of § 170.315 identified below is certified to either approach 1 (technically demonstrate) or approach 2 (system documentation) as follows:

| **If the Health IT Module includes capabilities for certification listed under:** | **It will need to be certified to approach 1 or approach 2 for each of the P&S certification criteria listed in the "approach 1" column** | |
|---|---|---|
| | **Approach 1** | **Approach 2** |
| § 170.315(a) | § 170.315(d)(1) (authentication, access control, and authorization), (d)(2) (auditable events and tamper resistance), (d)(3) (audit reports), (d)(4) (amendments), (d)(5) (automatic log-off), (d)(6)(emergency access), and (d)(7) (end-user device encryption) | For each applicable P&S certification criterion not certified for approach 1, there must be system documentation sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion. |
| § 170.315(b) | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) (integrity) | |
| § 170.315(c) | § 170.315(d)(1) through (d)(3) | |
| § 170.315(e) | § 170.315(d)(1) through (d)(3), (d)(5), and (d)(7) | |
| § 170.315(f) | § 170.315(d)(1) through (d)(3) and (d)(7) | |
| § 170.315(h) | § 170.315(d)(1) through (d)(3) | |
| § 170.315(i) | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | |

To illustrate approach 1 of privacy and security certification, if a Health IT Module is presented for certification to § 170.315(a)(5) ("demographics"), then the Health IT Module must also be certified to § 170.315(d)(1) through (7). We refer readers to Appendix A of this proposed rule for a listing of the P&S certification requirements for each 2015 Edition criterion under approach 1.

Because we have explicitly proposed which P&S certification criteria would be applicable to the associated criteria adopted in each regulatory text "first level paragraph" category and have also proposed approach 2, we have not proposed to permit the 2011 Edition policy of allowing for a criterion to be met through documentation that the criterion is inapplicable or would be technically infeasible for the Health IT Module to meet.

We seek comment on the overall clarity and feasibility of this approach.

2. Design and Performance (§ 170.315(g))

**Appendix A. 2015 Edition Health IT Certification Criteria**

| Proposed CFR Citation | Certification Criterion | Estimated Average Developmental Hours[270] Av. Low/Av. High | Proposed Privacy and Security Certification Requirements[271] (Approach 1) | Conditional Certification Requirements (§ 170.550) | Gap Certification Eligibility | Proposed Inclusion in 2015 Edition Base EHR Definition | Relationship to the Proposed CEHRT[272] Definition and Proposed EHR Incentive Programs Stage 3 Objectives |
|---|---|---|---|---|---|---|---|
| § 170.315 (a)(1) | Computerized Provider Order Entry (CPOE) – medications | 0/50 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3)<br>§ 170.315(g)(4)<br>§ 170.315(g)(8) | § 170.314(a)(1)<br>§ 170.314(a)(18) | Included[273] | Objective 4 |
| § 170.315 (a)(2) | CPOE – laboratory | 1,000/2,000 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3)<br>§ 170.315(g)(4)<br>§ 170.315(g)(8) | Not eligible | Included[274] | Objective 4 |
| § 170.315 (a)(3) | CPOE – diagnostic imaging | 0/50 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3)<br>§ 170.315(g)(4)<br>§ 170.315(g)(8) | § 170.314(a)(1)<br>§ 170.314(a)(20) | Included[275] | Objective 4 |
| § 170.315 (a)(4) | Drug-drug, Drug-allergy Interaction Checks for CPOE | 400/800 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3)<br>§ 170.315(g)(4)<br>§ 170.315(g)(8) | Not eligible | Not included | Objective 3 |
| § 170.315 (a)(5) | Demographics | 500/1,000 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3)<br>§ 170.315(g)(4)<br>§ 170.315(g)(8) | Not eligible | Included | No additional relationship beyond the Base EHR Definition |
| § 170.315 (a)(6) | Vital Signs, BMI, and Growth Charts | 614/922 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3)<br>§ 170.315(g)(4) | Not eligible | Not included | No relationship |

[270] Please see section VIII ("Regulatory Impact Statement") of the preamble for information on how estimated development hours were calculated. To note, certification to the 2014 Edition serves as a foundation for estimating costs. For unchanged certification criteria, in establishing our cost estimates for this proposed rule, we used burden hours multiplied by all health IT developers previously certified to the 2014 Edition version of the certification criteria to account for new entrants. These burden hour estimates are not estimates for development of a new product to meet one or more of these certification criteria. For certification criteria not associated with the EHR Incentive Programs Stage 3, there is a 60% reduction in burden hours. This reduction is due to our estimate that health IT developers would develop 1 product instead of 2.5 products to each of the certification criteria.

[271] We propose to require that an ONC-ACB must ensure that a Health IT Module presented for certification to any of the certification criteria that fall into the regulatory functional categories of § 170.315 for which privacy and security certification requirements apply either pursues approach 1 (detailed in the table) or approach 2: Demonstrate, through system documentation sufficiently detailed to enable integration, that the Health IT Module has implemented service interfaces for each applicable privacy and security certification criterion that enable the Health IT Module to access external services necessary to meet the privacy and security certification criterion.

[272] CMS' CEHRT definition would include the criteria adopted in the Base EHR definition. For more details on the CEHRT definition, please see the CMS EHR Incentive Programs proposed rule published elsewhere in this issue of the **Federal Register**.

[273] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[274] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

[275] Technology needs to be certified to § 170.315(a)(1), (a)(2), or (a)(3).

**Appendix A. 2015 Edition Health IT Certification Criteria**

| Proposed CFR Citation | Certification Criterion | Estimated Average Developmental Hours[270] Av. Low/Av. High | Proposed Privacy and Security Certification Requirements[271] (Approach 1) | Conditional Certification Requirements (§ 170.550) | Gap Certification Eligibility | Proposed Inclusion in 2015 Edition Base EHR Definition | Relationship to the Proposed CEHRT[272] Definition and Proposed EHR Incentive Programs Stage 3 Objectives |
|---|---|---|---|---|---|---|---|
| | | | | § 170.315(g)(8) | | | |
| § 170.315 (a)(7) | Problem List | 100/200 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Included | No additional relationship beyond the Base EHR Definition |
| § 170.315 (a)(8) | Medication List | 0/50 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | § 170.314(a)(6) | Included | No additional relationship beyond the Base EHR Definition |
| § 170.315 (a)(9) | Medication Allergy List | 0/50 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | § 170.314(a)(7) | Included | No additional relationship beyond the Base EHR Definition |
| § 170.315 (a)(10) | Clinical Decision Support | 600/1,200 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Included | Objective 3 |
| § 170.315 (a)(11) | Drug-formulary and Preferred Drug List Checks | 310/620 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 2 |
| § 170.315 (a)(12) | Smoking Status | 100/200 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Included | No additional relationship beyond the Base EHR Definition |
| § 170.315 (a)(13) | Image Results | 0/20 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(a)(12) | Not included | No relationship |
| § 170.315 (a)(14) | Family Health History | 100/200 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | CEHRT[276] |
| § 170.315 (a)(15) | Family Health History – pedigree | 500/1,200 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | CEHRT[277] |
| § 170.315 (a)(16) | Patient List Creation | 0/20 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(a)(14) | Not included | No relationship |
| § 170.315 (a)(17) | Patient-specific Education Resources | 600/1,200 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 5 |
| § 170.315 (a)(18) | Electronic Medication Administration Record | 0/20 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | § 170.314(a)(16) | Not included | No relationship |

[276] Technology needs to be certified to § 170.315(a)(14) or (a)(15).
[277] Technology needs to be certified to § 170.315(a)(14) or (a)(15).

**Appendix A. 2015 Edition Health IT Certification Criteria**

| Proposed CFR Citation | Certification Criterion | Estimated Average Developmental Hours[270] Av. Low/Av. High | Proposed Privacy and Security Certification Requirements[271] (Approach 1) | Conditional Certification Requirements (§ 170.550) | Gap Certification Eligibility | Proposed Inclusion in 2015 Edition Base EHR Definition | Relationship to the Proposed CEHRT[272] Definition and Proposed EHR Incentive Programs Stage 3 Objectives |
|---|---|---|---|---|---|---|---|
| § 170.315 (a)(19) | Patient Health Information Capture | 500/1,000 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | CEHRT Objective 6 |
| § 170.315 (a)(20) | Implantable Device List | 1,100/1,700 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Included | No additional relationship beyond the Base EHR Definition |
| § 170.315 (a)(21) | Social, Psychological, and Behavioral Data | 235/470 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (a)(22) | Decision Support – knowledge artifact | 394/788 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (a)(23) | Decision Support – service | 229/458 | § 170.315(d)(1) through (d)(7) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (b)(1) | Transitions of Care | 1,550/3,100 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8) | Not eligible | Included | Objective 7 |
| § 170.315 (b)(2) | Clinical Information Reconciliation and Incorporation | 600/1,200 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8) | Not eligible | Not included | Objective 7 |
| § 170.315 (b)(3) | Electronic Prescribing | 1,050/2,100 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 2 |
| § 170.315 (b)(4) | Incorporate Laboratory Tests and Values/Results | 313/626 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(3) § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (b)(5) | Transmission of Laboratory Test Reports | 360/720 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (b)(6) | Data Portability | 800/1,200 | § 170.315(d)(1) through (d)(3) and | § 170.315(g)(4) § 170.315(g)(6) | Not eligible | Included | No additional relationship beyond the Base EHR |

**Appendix A. 2015 Edition Health IT Certification Criteria**

| Proposed CFR Citation | Certification Criterion | Estimated Average Developmental Hours[270] Av. Low/Av. High | Proposed Privacy and Security Certification Requirements[271] (Approach 1) | Conditional Certification Requirements (§ 170.550) | Gap Certification Eligibility | Proposed Inclusion in 2015 Edition Base EHR Definition | Relationship to the Proposed CEHRT[272] Definition and Proposed EHR Incentive Programs Stage 3 Objectives |
|---|---|---|---|---|---|---|---|
| | | | (d)(5) through (d)(8) | § 170.315(g)(8) | | | Definition |
| § 170.315 (b)(7) | Data Segmentation for Privacy – send | 450/900 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (b)(8) | Data Segmentation for Privacy – receive | 450/900 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (b)(9) | Care Plan | 300/500 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (c)(1) | Clinical Quality Measures – record and export | 200/500 | § 170.315(d)(1) through (d)(3) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Included | CEHRT |
| § 170.315 (c)(2) | Clinical Quality Measures – import and calculate | 0/200 | § 170.315(d)(1) through (d)(3) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (c)(3) | Reserved for Clinical Quality Measures - record | Reserved | § 170.315(d)(1) through (d)(3) | § 170.315(g)(4) § 170.315(g)(8) | Reserved | Reserved | Reserved[278] |
| § 170.315 (c)(4) | Clinical Quality Measures – filter | 316/632 | § 170.315(d)(1) through (d)(3) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (d)(1) | Authentication, Access Control, Authorization | 0/50 | Not applicable (N/A) | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(d)(1) | Not included | No relationship |
| § 170.315 (d)(2) | Auditable Events and Tamper-resistance | 0/50 | N/A | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(d)(2) | Not included | No relationship |
| § 170.315 (d)(3) | Audit Report(s) | 0/50 | N/A | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(d)(3) | Not included | No relationship |
| § 170.315 (d)(4) | Amendments | 0/50 | N/A | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(d)(4) | Not included | No relationship |
| § 170.315 | Automatic Access Time-out | 0/50 | N/A | § 170.315(g)(4) | § 170.314(d)(5) | Not included | No relationship |

[278] As discussed in the preamble for the "clinical quality measures – report" criterion, additional CQM certification policy may be proposed in or with CMS payment rules in CY15. As such, additional CQM certification criteria may be proposed for the Base EHR and/or CEHRT definitions.

**Appendix A. 2015 Edition Health IT Certification Criteria**

| Proposed CFR Citation | Certification Criterion | Estimated Average Developmental Hours[270] Av. Low/Av. High | Proposed Privacy and Security Certification Requirements[271] (Approach 1) | Conditional Certification Requirements (§ 170.550) | Gap Certification Eligibility | Proposed Inclusion in 2015 Edition Base EHR Definition | Relationship to the Proposed CEHRT[272] Definition and Proposed EHR Incentive Programs Stage 3 Objectives |
|---|---|---|---|---|---|---|---|
| (d)(5) | | | | § 170.315(g)(8) | | | |
| § 170.315 (d)(6) | Emergency Access | 0/50 | N/A | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(d)(6) | Not included | No relationship |
| § 170.315 (d)(7) | End-User Device Encryption | 0/50 | N/A | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(d)(7) | Not included | No relationship |
| § 170.315 (d)(8) | Integrity | 0/50 | N/A | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(d)(8) | Not included | No relationship |
| § 170.315 (d)(9) | Accounting of Disclosures | 0/20 | N/A | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(d)(9) | Not included | No relationship |
| § 170.315 (e)(1) | View, Download, and Transmit to 3rd Party | 1,000/2,000 | § 170.315(d)(1) through (d)(3), (d)(5), and (d)(7) | § 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8) | Not eligible | Not included | Objective 5 Objective 6 |
| § 170.315 (e)(2) | Secure Messaging | 0/50 | § 170.315(d)(1) through (d)(3), (d)(5), and (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | § 170.314(e)(3) | Not included | Objective 6 |
| § 170.315 (f)(1) | Transmission to Immunization Registries | 680/1,360 | § 170.315(d)(1) through (d)(3) and (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 8[279] |
| § 170.315 (f)(2) | Transmission to Public Health Agencies – syndromic surveillance | 480/960 | § 170.315(d)(1) through (d)(3) and (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 8 |
| § 170.315 (f)(3) | Transmission to Public Health Agencies – reportable laboratory tests and values/results | 520/1,040 | § 170.315(d)(1) through (d)(3) and (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 8 |
| § 170.315 (f)(4) | Transmission to Cancer Registries | 500/1,000 | § 170.315(d)(1) through (d)(3) and (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 8 |
| § 170.315 (f)(5) | Transmission to Public Health Agencies – case reporting | 500/1,000 | § 170.315(d)(1) through (d)(3) and (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 8 |

[279] For the public health certification criteria in § 170.315(f), technology would only need to be certified to those criteria that are required to meet the options the provider intends to report in order to meet the proposed Objective 8: Public Health and Clinical Data Registry Reporting.

**Appendix A. 2015 Edition Health IT Certification Criteria**

| Proposed CFR Citation | Certification Criterion | Estimated Average Developmental Hours[270] Av. Low/Av. High | Proposed Privacy and Security Certification Requirements[271] (Approach 1) | Conditional Certification Requirements (§ 170.550) | Gap Certification Eligibility | Proposed Inclusion in 2015 Edition Base EHR Definition | Relationship to the Proposed CEHRT[272] Definition and Proposed EHR Incentive Programs Stage 3 Objectives |
|---|---|---|---|---|---|---|---|
| § 170.315 (f)(6) | Transmission to Public Health Agencies – antimicrobial use and resistance reporting | 500/1,000 | § 170.315(d)(1) through (d)(3) and (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 8 |
| § 170.315 (f)(7) | Transmission to Public Health Agencies – health care surveys | 500/1,000 | § 170.315(d)(1) through (d)(3) and (d)(7) | § 170.315(g)(4) § 170.315(g)(8) | Not eligible | Not included | Objective 8 |
| § 170.315 (g)(1) | Automated Numerator Recording | 400/800 | N/A | § 170.315(g)(4) | Fact-specific | Not included | CEHRT |
| § 170.315 (g)(2) | Automated Measure Calculation | 600/1,200 | N/A | § 170.315(g)(4) | Fact-specific | Not included | CEHRT |
| § 170.315 (g)(3) | Safety-Enhanced Design | 300/600 | N/A | N/A | Fact-specific | Not included | No relationship |
| § 170.315 (g)(4) | Quality Management System | 400/800 | N/A | N/A | Not eligible | Not included | No relationship |
| § 170.315 (g)(5) | Accessibility Technology Compatibility | 800/1400 | N/A | N/A | Not eligible | Not included | No relationship |
| § 170.315 (g)(6) | Consolidated CDA Creation Performance | 400/1,000 | N/A | N/A | Not eligible | Not included | No relationship |
| § 170.315 (g)(7) | Application Access to Common Clinical Data Set | 500/1,000 | N/A | § 170.315(g)(4) § 170.315(g)(6) § 170.315(g)(8) | Not eligible | Included | Objective 5 Objective 6 |
| § 170.315 (g)(8) | Accessibility-Centered Design | 50/100 | N/A | N/A | Not eligible | Not included | No relationship |
| § 170.315 (h)(1) | Direct Project | 0/50 | § 170.315(d)(1) through (d)(3) | § 170.315(b)(1) § 170.315(g)(4) § 170.315(g)(8) | § 170.314 (b)(1)(i)(A) and § 170.314 (b)(2)(ii)(A) § 170.314(h)(1) | Included[280] | No relationship beyond the Base EHR Definition |
| § 170.315 (h)(2) | Direct Project, Edge Protocol, and XDR/XDM | 0/50 | § 170.315(d)(1) through (d)(3) | § 170.315(g)(4) § 170.315(g)(8) | § 170.314 (b)(1)(i)(B), § 170.314 | Included[282] | No relationship beyond the Base EHR Definition |

[280] Technology needs to be certified to § 170.315(h)(1) or (h)(2).

**Appendix A. 2015 Edition Health IT Certification Criteria**

| Proposed CFR Citation | Certification Criterion | Estimated Average Developmental Hours[270] Av. Low/Av. High | Proposed Privacy and Security Certification Requirements[271] (Approach 1) | Conditional Certification Requirements (§ 170.550) | Gap Certification Eligibility | Proposed Inclusion in 2015 Edition Base EHR Definition | Relationship to the Proposed CEHRT[272] Definition and Proposed EHR Incentive Programs Stage 3 Objectives |
|---|---|---|---|---|---|---|---|
| | | | | | (b)(2)(ii)(B), and § 170.314(b)(8)[281]<br>170.314(b)(8)[283] and 170.314(h)(2) | | |
| § 170.315 (h)(3) | SOAP Transport and Security Specification and XDR/XDR for Direct Messaging | 0/20 | § 170.315(d)(1) through (d)(3) | § 170.315(g)(4)<br>§ 170.315(g)(8) | § 170.314 (b)(1)(i)(C) and § 170.314 (b)(2)(ii)(C)<br>§ 170.314(h)(3) | Not included | No relationship |
| § 170.315 (h)(4) | Healthcare Provider Directory – query request | 120/240 | § 170.315(d)(1) through (d)(3) | § 170.315(g)(4)<br>§ 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (h)(5) | Healthcare Provider Directory – query response | 120/240 | § 170.315(d)(1) through (d)(3) | § 170.315(g)(4)<br>§ 170.315(g)(8) | Not eligible | Not included | No relationship |
| § 170.315 (j)(1) | Electronic Submission of Medical Documentation | 1000/200 | § 170.315(d)(1) through (d)(3) and (d)(5) through (d)(8) | § 170.315(g)(4)<br>§ 170.315(g)(6)<br>§ 170.315(g)(8) | Not eligible | Not included | No relationship |

[FR Doc. 2015-06612 Filed: 3/20/2015 03:00 pm; Publication Date: 3/30/2015]

[282] Technology needs to be certified to § 170.315(h)(1) or (h)(2).
[281] Technology must have been certified to both edge protocol methods specified by the standard in § 170.202(d) to be gap certification eligible.
[283] Technology must have been certified to both edge protocol methods specified by the standard in § 170.202(d) to be gap certification eligible.