The Office of the National Coordinator for
Health Information Technology

## 2015 Edition Privacy and Security Certification Framework

| **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),<br>(d)(2) (auditable events and tamper resistance),<br>(d)(3) (audit reports),<br>(d)(4) (amendments),<br>(d)(5) (automatic log-off),<br>(d)(6) (emergency access), and<br>(d)(7) (end-user device encryption) | For each applicable P&S certification criterion not certified for approach 1, the health IT developer may certify for the criterion using system documentation sufficiently detailed to enable integration with external services necessary to meet the 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) and (d)(5) | |
| § 170.315(e)(1) | § 170.315(d)(1) through (d)(3), (d)(5), (d)(7), and (d)(9)(trusted connection) | |
| § 170.315(e)(2) and (3) | § 170.315(d)(1) through (d)(3), (d)(5), and (d)(9) | |
| § 170.315(f) | § 170.315(d)(1) through (d)(3) and (d)(7) | |
| § 170.315(g)(7), (8) and (9) | § 170.315(d)(1) and (d)(9); and (d)(2) or (d)(10) (auditing actions on health information) | |
| § 170.315(h) | § 170.315(d)(1) through (d)(3) | |

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 paragraph” category of § 170.315 (e.g. § 170.315(a)) identified in the table above is certified to either Approach 1 (technically demonstrate) or Approach 2 (system documentation).

We clarify that of the adopted 2015 Edition certification criteria, only the privacy and security criteria specified in § 170.315(g)(1) through (6) are exempt from the privacy and security certification framework due to the capabilities included in these criteria, which do not implicate privacy and security concerns.

In order to be issued a certification, a Health IT Module would only need to be tested once to each applicable privacy and security criterion identified as part of Approach 1 or Approach 2 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, except for the certification of a Health IT Module to § 170.315(e)(1) “VDT” and (e)(2) “secure messaging.”  For each of these criteria, a Health IT Module must be separately tested to § 170.315(d)(9) because of the specific capabilities for secure electronic transmission and secure electronic messaging included in each criterion, respectively.