DRAFT EXAMPLES OF HOW APPLICABILITY OF PRIVACY AND SECURITY CRITERIA MIGHT BE REPRESENTED

Security Criteria As Worded in 2014 Edition	Module Security Applicability Statement(s)	Comments on Criterion Wording
Authentication, access control, authorization: Authentication, access control, and authorization. (i) Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed; and (ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the EHR technology.	**If the module has human users,** demonstrate that the module: — verifies against a unique identifier(s) (e.g., username or number) that the person seeking access to electronic health information is the one claimed — establishes the type of access and the actions permitted by that user	This criterion should accommodate the ability to authenticate, authorize and control access to SYSTEM users, not just human users.
Auditable events, tamper-resistance: (i) Record actions. EHR technology must be able to: (A) Record actions related to electronic health information in accordance with the standard specified in **§170.210(e)(1)**; (B) Record the audit log status (enabled or disabled) in accordance with the standard specified in § 170.210(e)(2) unless it cannot be disabled by any user; and (C) Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by EHR technology in accordance with the standard specified in § 170.210(e)(3) unless the EHR technology prevents electronic health information from being locally stored on end-user devices (see 170.314(d)(7) of this section). (ii) Default setting. EHR technology must be set by default to perform the capabilities specified in paragraph (d)(2)(i)(A) of this section and, where applicable, paragraphs (d)(2)(i)(B) or (C), or both paragraphs (d)(2)(i)(B) and (C). (iii) When disabling the audit log is permitted. For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that EHR technology permits to be disabled, the ability to do so must be restricted to a limited set of identified users. (iv) Audit log protection. Actions and statuses recorded in accordance with paragraph (d)(2)(i) of this section must not be capable of being changed, overwritten, or deleted by the EHR technology. (v) Detection. EHR technology must be able to detect whether the audit log has been altered.	**If the module captures, stores, enables access, or is used to disclose electronic health information maintained in EHR,** demonstrate that module: — records ***applicable*** actions (specified in §170.210(e)(1)) — records audit log status (enabled/disabled) — restricts the ability of users to disable the audit function to a limited set of users — defaults to perform these capabilities — cannot delete contents of log — detect when log has been altered **If the module encrypts local PHI data,** demonstrate that the module: — records the encryption status of the locally stored PHI data	Considering the module certification approach, it is important to note that not all ASTM requirements apply to all modules. Suggest insert “applicable” in criterion wording.
Audit report(s): Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the data specified in the standards at § 170.210(e).	**If the module maintains a security audit log,** demonstrate that the module: — enables the user to create an audit report	

Security Criteria As Worded in 2014 Edition	Module Security Applicability Statement(s)	Comments on Criterion Wording
Amendments: Enable a user to electronically select the record affected by a patient's request for amendment and perform the capabilities specified in paragraphs (d)(4)(i) or (ii) of this section. (i) Accepted amendment. For an accepted amendment, append the amendment to the affected record or include a link that indicates the amendment's location. (ii) Denied amendment. For a denied amendment, at a minimum, append the request and denial of the request to the affected record or include a link that indicates this information's location.	**If the module supports patient-requested amendments to electronic health information maintained in EHR,** demonstrate that the module: — allows an authenticated user to – append accepted amendment (or link) to patient record – append the request and denial of the request to the affected record	
Automatic Log-off: Prevent a user from gaining further access to an electronic session after a predetermined time of inactivity.	**If the module requires authentication of human users,** demonstrate that the module: — prevents a user from gaining access to an electronic session after a predetermined time of inactivity	No user should gain access without logging (back) into the system. Thus, we suggest deletion of "further."
Emergency Access: Permit an identified set of users to access electronic health information during an emergency	**If the module allows human users access to electronic health information, AND If the module performs functions supporting the purpose of delivering patient care,** demonstrate that the module: — supports emergency access by an identified set of users	
End-user device encryption: EHR technology that is designed to locally store electronic health information on end-user devices must encrypt the electronic health information stored on such devices after use of EHR technology on those devices stops	**If the module stores electronic data at rest in a locally accessible data store on an end-user device after use of EHR technology on those devices stops,** demonstrate that the module: — encrypts any residual data — is set by default to perform this capability and, the ability to change the configuration is either absent or restricted to a limited set of identified users **If the module is designed to prevent storage of electronic data at rest in a locally accessible data store on end-user devices after use of EHR technology on those devices stops,** demonstrate that the module: — does not store residual data	
Integrity: (i) Create a message digest in accordance with the standard specified in § 170.210(c). (ii) Verify in accordance with the standard specified in § 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered.	**If the module transmits PHI,** demonstrate that the module: — creates a message digest in accordance with the standard specified in §170.210(c) **If the module receives PHI**, demonstrate that the module: — upon receipt of a message that has been integrity-protected in accordance with the standard specified in §170.210(c), the module is able to verify that the health information has not been altered	