# Test Criteria: 170.315.d.2 Auditable Events and Tamper-resistance

|  |  |
| --- | --- |
| **Testing Result** |  |
| Participant and Product-with-version |  |
| Setting (Ambulatory or Inpatient) |  |
| Test Proctor |  |
| Test Date |  |
| Test Result | Pass:  Fail:  No Attempt: |
| Error Description (if applicable) |  |
| Modifications to Product Under Test |  |
| Additional Software Used |  |
| Additional Proctor Notes |  |

### Overview

In this document you will find:

* [Test Data and Test Tools](#_Test_Data_and)
* [Standards Support](#_Demonstrate_Standards_Support)
* [Drummond Test Report (Instructions, Expected Results, Points to Remember)](#_170.315(d)(2)(i)(A)_Record_actions)
* [Test Procedures](#_Test_Procedures)
* [Appendix A: Testing Guide](#_Appendix_A:_Testing)
* [Appendix B: ONC Criteria](#_Appendix_B:_ONC)

### Version of ONC Test Method

1.1

### Scope of Proctoring Sheet

The ONC test method associated with this criterion is the only approved test method for EHR Meaningful Use certification. This Proctoring Sheet is not a replacement test method but a test procedure document for performing the ONC test method and recording the results. Proctoring Sheet describe test data, test criteria and expected results. It is assumed the Health IT developer or Participant Under Test is familiar with the associated ONC test method.

# Robustness and Reliability Requirement

To satisfy the module criteria, it is expected that the Product-Under-Test is able to complete the testing requirements reliably, including repeat testing with the same result without error, and with a satisfactory level of robustness. This includes unexpected error messages produced through normal operation, multiple unintended restarts of the application or any other “buggy” facets of the product displayed while testing. These errors are record in the Additional Proctor Notes of the proctor sheet. Lack of reliability and robustness of design will result in failure of the module.

# Test Data and Tools

|  |  |
| --- | --- |
| **Test Data Source:** | ONC-Supplied  DG-Supplied:  Developer-Supplied: |
| **Pre-Test Data Setup:**  Not applicable. | |
| **Test Data:**  The Test Proctor may rely on data entered for other modules during the test event. If unavailable, or at the Proctor’s discretion, new test data may be required to be entered while testing this module. | |
| **Test Tools:**  Not applicable. | |

# Demonstrate Standards Support

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:** Record actions related to electronic health information, audit log status, and encryption of end-user devices according to the specified sections of the ASTM E2147-01 standard using the NTP standard for date and time. | |

|  |  |  |
| --- | --- | --- |
|  | **Standard** |  |
|  | §170.210(e)(1) | 1. The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standard specified at §170.210(h) and changes to users privileges when health IT is in use. 2. The date and time must be recorded in accordance with the standard specified at §170.210(g). |
|  | §170.210(e)(2) | 1. The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the audit log status is changed. 2. The date and time each action occurs in accordance with the standard specified at §170.210(g). |
|  | §170.210(e)(3) | The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at §170.210(g). |
|  | §170.210(g) | Synchronized clocks. The date and time recorded utilize a system clock that has been synchronized following [(RFC 1305) Network Time Protocol](http://www.rfc-editor.org/info/rfc1305), (incorporated by reference in §170.299) or [(RFC 5905) Network Time Protocol Version 4](http://www.rfc-editor.org/info/rfc5905), (incorporated by reference in §170.299). |
|  | §170.210(h) | Audit log content [ASTM E2147-01 (Reapproved 2009)](http://www.astm.org/Standards/E2147.htm), (incorporated by reference in §170.299). |

# 170.315(d)(2)(i)(A) Record actions

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **P&S applies to all criteria:** | YES:  NO: |
| **If not, list applicable criteria:** |  |
| **Instructions:** Health IT module demonstrates synchronization to a configured NTP server. The audit log records actions related to electronic health information, audit log status, and encryption status. | |
| **Expected Test Result:**   * Record actions related to electronic health information in accordance with the standard specified in §170.210(e)(1). * All actions recorded by the audit log shall include:  1. Date and Time (utilizing a system clock synchronized following the NTP or NTP v4); 2. Patient Identification; 3. User Identification; 4. Type of Action (additions, deletions, changes, queries, print, copy), specifying inquiry, any changes made (if any), and a description of any data deleted (if any); and 5. Identification of patient data accessed  * Health IT module system time is synchronized within five seconds of the NTP configured ITS server. * If applicable, the EHR time is within five seconds of the health IT module system time or the NTP configured ITS server. | |
| **Points to Remember:**   * The certification criterion requires actions initiated by the user from within the health IT interface to be tracked in the audit log. This includes: *additions, deletions, changes, queries, print, copy,* and *access to patient health information including emergency access events.* * Any changes to a user’s privileges must be captured to meet this criterion (e.g., user account creation, user switches roles and new privileges are assigned, revoking privileges, account disabling, etc.). * Actions and information are intended to be captured in a manner that supports the forensic reconstruction of the sequence of changes to a patient’s chart. * Only those sections specified from section 7 of ASTM E2147-01 are the minimum required for certification. * In regards to P&S requirements for modules (g.8) and (g.9), the audit record should be able to distinguish the specific user who accessed the data using a third-party application through the certified API. * Testing assumes the operating system synchronizes to the NTP server and the Health IT Module then synchronizes to the operating system; however, the Heath IT Module could synchronize directly to the NTP server. The Health IT Module may use either method to demonstrate that the synchronization has occurred. Use of internal NTP servers are allowed, but the Health IT Module must demonstrate that the internal servers are synced to a NIST timeserver for accuracy. * See “[EHR Test-128] Privacy and Security Framework” document provided by Drummond Group to verify instructions on submitting required P&S attestation. | |

### Test Procedures

**1.1 NTP Test**

|  |  |
| --- | --- |
|  | Configure the HIT module’s operating system NTP server to an ITS server:  NIST Timer Server: <NIST Time Server> |
|  | Synchronize the HIT module operating system NTP server to the ITS server. |
|  | Verify that NTP server never queries the time server more than once every 4 seconds. |
|  | The HIT module operating system display time is accurate within 5 seconds of the NIST time server. |
|  | HIT module display time is accurate within 5 seconds of the operating system time. (Alternative)  HIT module display time is accurate within 5 seconds of the NIST time server. (Alternative) |
|  | Time Service (ITS):  NTP version:  NTPv3  NTPv4 |
|  | Proctor records the NIST Internet Time Service (ITS) Server used to demonstrate synchronization.  **NIST ITS Server:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

<INSERT SCREEN SHOTS - NTP Configuration>

<INSERT SCREEN SHOTS - NTP Logs>

**1.2 Record Actions**

|  |  |
| --- | --- |
|  | Authorized user logs in performs each action in order to generate an audit log entry in accordance with standard §170.210(e)(1):   * **Additions** * **Deletions** * **Changes** * **Queries** * **Print** * **Copy** * **Changes to user privileges** * **Access to patient information, including emergency access events** |
|  | For all permissible actions, the audit log function records the following data:   * **Date and time of event**, synchronized according to NTPv3 or NTPv4 in accordance with the standard specified in §170.210(g); * **Patient identification**; * **User identification**; * **Type of action** (additions, deletions, changes, queries, print, copy), specifying inquiry, any changes made (if any), and a description of any data deleted (if any); **and** * **Identification of the patient data that are accessed**. |

<INSERT SCREEN SHOTS>

**1.3 Privacy and Security Attestation**

|  |  |
| --- | --- |
|  | Health IT Developer submits Privacy and Security Framework document attesting to the approach used for certification testing. Additionally, attestation must specify if the criteria demonstrated in this test event applies to *all* certified modules or only specific modules. See the “[EHR Test-128] Privacy Security Framework” document provided by Drummond Group. |
|  | For any action not supported by the health IT module, developer attests to the inability to demonstrate and is not subject to testing. Refer to framework document above for attestation template. |

<ATTACH or INSERT LINK TO DOCUMENTATION>

# 170.315(d)(2)(i)(B) Audit Log Status Disabling (Conditional)

# 170.315(d)(2)(i)(C) Encryption Status Disabling (Conditional)

# 170.315(d)(2)(iii) Disabling by Limited Set of Users

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Disabling permitted?** | YES:  NO: |
| **Instructions:** The audit log records the audit log status and/or the encryption status. | |
| **Expected Test Result:**   * 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. * If the audit log can be disabled, the health IT module records audit log status changes in accordance with standard specified at §170.210(e)(2). * Record the encryption status (enabled or disabled) of electronic health information locally stored on end-user devices by technology in accordance with the standard specified in § 170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices. * If electronic health information can be locally stored on end user devices, the health IT module records when the encryption status, by the technology, changes. Status change should be logged in accordance with standard specified in §170.210(e)(3). * If disabling of the audit log and/or encryption status is permitted, health IT module shall log the status change by recording:  1. Date and time, synchronized according to NTPv3 or NTPv4 in accordance with the standard specified in §170.210(g); 2. User identification; and 3. Actions that occurred  * Where the health IT module permits disabling, the capability to do so is restricted to a limited set of users for each auditing function:  1. Record actions; 2. Record the audit log status; and 3. Record encryption status. | |
| **Points to Remember:**   * This section should be tested only if the audit log can be disabled and/or the encryption can be disabled. * **If the health IT module does not permit disabling** of the audit log or encryption status, the health IT developer will submit documentation attesting to these inabilities and will not be subject to testing this section. Refer to the “[EHR Test-128] Privacy Security Framework” document provided by Drummond Group for attestation template. | |

### Test Procedures

**2.1 Audit Log Status – Audit Log cannot be disabled**

|  |  |
| --- | --- |
|  | If audit log cannot be disabled, health IT developer submits documentation attesting to these inabilities and will not be subject to testing this section. Refer to “[EHR Test-128] Privacy Security Framework” provided by Drummond Group for attestation template. |

<ATTACH or INSERT LINK TO DOCUMENTATION>

**2.2 Audit Log Status – Audit Log can be disabled**

|  |  |
| --- | --- |
|  | If audit log status can be disabled, verify the limited set of users authorized to disable. |
|  | Authorized user disables audit log. Health IT module records the change in audit log status from ‘enabled’ to ‘disabled’ (and vice versa) and logs the status change in accordance with standard specified in §170.210(e)(2), by recording:   * **date and time**, synchronized according to NTPv3 or NTPv4; * **user identification**; and * **which action(s) occurred** |
|  | Unauthorized user attempts to disable audit log status but is unable to do so. |
|  | If the Health IT Module permits disabling of **record actions** (actions in section 1.2 above), demonstrate that the capability to do so is restricted to a limited set of users. |

<INSERT SCREEN SHOTS>

**2.3 Encryption Status – Encryption Status cannot be disabled**

|  |  |
| --- | --- |
|  | If encryption status cannot be disabled, or if electronic health information cannot be stored locally by the technology, health IT developer submits documentation attesting to these inabilities and will not be subject to testing this section. Refer to the “[EHR Test-128] Privacy Security Framework” provided by Drummond Group for attestation template. |

<ATTACH or INSERT LINK TO DOCUMENTATION>

**2.4 Encryption Status – Encryption Status can be disabled**

|  |  |
| --- | --- |
|  | If encryption status can be disabled, verify the limited set of users authorized to disable. |
|  | Authorized user disables encryption status. Health IT module records the change in encryption status from ‘enabled’ to ‘disabled’ (and vice versa) and logs the status change in accordance with standard specified in §170.210(e)(2), by recording:   * **date and time**, synchronized according to NTPv3 or NTPv4 in accordance with the standard specified in § 170.210(g); * **user identification**; and * **which action(s) occurred** |
|  | Unauthorized user attempts to disable encryption status but is unable to do so. |

<INSERT SCREEN SHOTS>

# 170.315(d)(2)(iv) Protect Audit Log

# 170.315(d)(2)(v) Detection of Audit Log Alteration

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **Instructions:** Health IT developer provides documentation describing how the health IT module protects the audit log and how alterations to the audit log are detected. | |
| **Expected Test Result:**   * Submit signed attestation documents to the Test Proctor describing how the health IT module protects the audit log and how alterations to the audit log are detected. | |
| **Points to Remember:**   * Protect audit log (d)(2)(iv) would not prohibit an organization from making a policy decision to delete or purge audit logs after a legal retention period. Rather it focuses only on the prohibition of health IT to delete an audit log as a condition of certification. * Detection of Audit Log Alteration (d)(2)(v) requires health IT to be able to determine whether activity outside of its control has in some way altered the audit log (e.g., that the operating system was exploited to modify the health IT’s database). * The use of hashing algorithms with strength equal or greater than SHA-2 as specified in FIPS 180-4 (Secure Hash Standard) to determine whether the audit log has been altered is strongly recommended. * Refer to the “[EHR Test-128] Privacy Security Framework” document provided by Drummond Group for attestation template. | |

### Test Procedures

**3.1 Protect Audit Log and Detect Audit Log Alteration**

|  |  |
| --- | --- |
|  | Using the “[EHR Test-128] Privacy Security Framework” document, health IT developer attests how the audit log is protected from having the following data elements from being changed, overwritten, or deleted by the health IT module:   * + Recording of actions related to electronic health information;   + Recording of audit log status; and   + Recording of encryption status. |
|  | Health IT developer attests to how alterations to an audit log are detected. |
|  | Proctor reviews attestation document and verifies the health IT module protects the outlined items from being changed, overwritten, or deleted from the audit log and that alterations to an audit log are successfully detected. |

<ATTACH or INSERT LINK TO DOCUMENTATION>

# Appendix A: Testing Guide

*This appendix contains more details and background on the testing requirements, including explanation on underlying standards, notable issues and best practice suggestions.*

Rev 01-Nov-2016 Additions

* Synchronized system clock based on the specifications in RFC 1305 (Network Time Protocol v3) or RFC 5905 (Network Time Protocol v4).
* Acceptable time servers are referenced here (<http://tf.nist.gov/tf-cgi/servers.cgi>) and copied below for quick reference.

**Note: All users should ensure that their software *NEVER* queries a server more frequently than once every 4 seconds. Systems that exceed this rate will be refused service. In extreme cases, systems that exceed this limit may be considered as attempting a denial-of-service attack.**

|  |  |  |
| --- | --- | --- |
| **Name** | **IP Address** | **Location** |
| time-a.nist.gov | 129.6.15.28 | NIST, Gaithersburg, Maryland |
| time-b.nist.gov | 129.6.15.29 | NIST, Gaithersburg, Maryland |
| time-c.nist.gov | 129.6.15.30 | NIST, Gaithersburg, Maryland |
| time-d.nist.gov | 2610:20:6F15:15::27 | NIST, Gaithersburg, Maryland |
| nist1-macon.macon.ga.us | 98.175.203.200 | Macon, Georgia |
| wolfnisttime.com | 66.199.22.67 | Wolf-Tek, Birmingham, Alabama |
| nist.netservicesgroup.com | 64.113.32.5 | Southfield, Michigan |
| nisttime.carsoncity.k12.mi.us | 198.111.152.100 | Carson City, Michigan |
| nist1-lnk.binary.net | 216.229.0.179 | Lincoln, Nebraska |
| wwv.nist.gov | 24.56.178.140 | WWV, Fort Collins, Colorado |
| time-a.timefreq.bldrdoc.gov | 132.163.4.101 | NIST, Boulder, Colorado |
| time-b.timefreq.bldrdoc.gov | 132.163.4.102 | NIST, Boulder, Colorado |
| time-c.timefreq.bldrdoc.gov | 132.163.4.103 | NIST, Boulder, Colorado |
| time.nist.gov | global address for all servers | Multiple locations |
| utcnist.colorado.edu | 128.138.140.44 | University of Colorado, Boulder |
| utcnist2.colorado.edu | 128.138.141.172 | University of Colorado, Boulder |
| time-nw.nist.gov | 131.107.13.100 | Microsoft, Redmond, Washington |
| nist-time-server.eoni.com | 216.228.192.69 | La Grande, Oregon |
| nist-time-server.eoni.com | 2607:f248::45 |  |

Rev 01-May-2016 Additions

* “Copy” can encompass a variety of actions, including extracting data from the health IT. Copy actions originating from within the health IT interface (e.g., exporting or downloading a copy of electronic health information from the health IT) are required to be tracked in the audit log.
* The copy and paste functions of Microsoft Windows originate outside of the health IT environment and are thus outside the scope of certification. Copy actions originating from within the health IT interface (e.g., exporting or downloading a copy of electronic health information from the health IT) are required to be tracked in the audit log.

Rev 01-Mar-2016 Additions

* Demonstration of the ability to use NIST time servers is required for certification, however vendors are not required to use NIST servers post certification.
* Information related to the required actions (additions, deletions, changes, queries, print, and copy) must be recorded in the audit log, however the certification criterion is not prescriptive to the method by which this is achieved and does not place limitations on the format in which this information is presented in the audit log.
* Only those sections specified from section 7 of ASTM E2147-01 are the minimum required for certification.

# Appendix B: ONC Criteria and Standards

*This appendix contains copy of the relevant ONC criteria and standards for this proctor sheet as a reference. In the event of a discrepancy with the ONC Final Rule, the ONC Final Rule takes precedence.*

**§170.315(d)(2) *Auditable events and tamper-resistance*—(**i) *Record actions.* 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 technology in accordance with the standard specified in § 170.210(e)(3) unless the technology prevents electronic health information from being locally stored on end-user devices.

(ii) *Default setting.* 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) and (d)(2)(i)(C) of this section.

(iii) *When disabling the audit log is permitted.* For each capability specified in paragraphs (d)(2)(i)(A) through (C) of this section that technology permits to be disabled, the ability to do so must be restricted to a limited set of 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 technology.

(v) *Detection.* Technology must be able to detect whether the audit log has been altered.

**§ 170.210 Standards for health information technology to protect electronic health information created, maintained, and exchanged.**

1. Record actions related to electronic health information, audit log status, and encryption of end-user devices.
   * 1. The audit log must record the information specified in sections 7.2 through 7.4, 7.6, and 7.7 of the standard specified at §170.210(h) when EHR technology is in use.
     2. The date and time must be recorded in accordance with the standard specified at §170.210(g).
     3. The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the audit log status is changed.
     4. The date and time each action occurs in accordance with the standard specified at §170.210(g).
   1. The audit log must record the information specified in sections 7.2 and 7.4 of the standard specified at §170.210(h) when the encryption status of electronic health information locally stored by EHR technology on end-user devices is changed. The date and time each action occurs in accordance with the standard specified at §170.210(g).
2. *Synchronized clocks.* The date and time recorded utilize a system clock that has been synchronized following (RFC 1305) Network Time Protocol, (incorporated by reference in §170.299) or (RFC 5905) Network Time Protocol Version 4, (incorporated by reference in §170.299).
3. *Audit log content.* ASTM E2147-01(Reapproved 2009), (incorporated by reference in §170.299)

# Change Log

|  |  |
| --- | --- |
| Revision | Change Description |
| 01-Nov-2016 | Added test step for proctor to record NIST ITS Server. Added list of NIST time servers in Appendix A. |
| 01-Oct-2016 | Updated “type of action” to align with ONC test procedure and removed explanation of “pointer” from Appendix A. |
| 01-Aug-2016 | Added field to indicate if audit log or encryption disabling permitted. |
| 01-July-2016 | Added reference to the required “[EHR Test-128] Privacy Security Framework” attestation template provided by Drummond Group. Removed Appendix C and moved template to “[EHR Test-128] Privacy Security Framework” document. |
| 01-Jun-2016 | Added text boxes to indicate if this P&S module applies to all certified criteria and reference to the attestation based on “Privacy and Security Framework” document. Split sections 2.1-2.4 to distinguish disabling capabilities. |
| 01-May-2016 | Removed step to “log into patient record” for section 1.2. Added clarification for user-initiated actions under “Points to Remember”. Added NTP Test procedure (section 1.1). |
| 01-Apr-2016 | Added expected result “identification of patient data accessed” under “Record Actions” section. Re-aligned expected result of recording audit log status and encryption status under their respective sections. |
| 01-Mar-2016 | Initial Release. |
|  |  |

**About Drummond Group LLC**

Drummond Group LLC is a global software test and certification lab that serves a wide range of vertical industries.  In healthcare, Drummond Group tests and certifies Controlled Substance Ordering Systems (CSOS), Electronic Prescription of Controlled Substances (EPCS) software and processes, and Electronic Health Records (EHRs) – designating the trusted test lab as the only third-party certifier of all three initiatives designed to move the industry toward a digital future. Founded in 1999, and accredited for the Office of the National Coordinator Health IT Certification Program as an Authorized Certification Body (ACB) and an Authorized Test Lab (ATL), Drummond Group continues to build upon its deep experience and expertise necessary to deliver reliable and cost-effective services. For more information, please visit <http://www.drummondgroup.com> or email [ehr@drummondgroup.com](mailto:ehr@drummondgroup.com)

END OF DOCUMENT