# Test Criteria: 170.315.d.3 Audit Reports

|  |  |
| --- | --- |
| **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)(3)_Create_and)
* [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:  Not Applicable: |
| **Instructions:** Generate an audit report with 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 user privileges when health IT is in use.   (ii) 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 with 2. The date and time must be recorded 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) | 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) | [ASTM E2147-01 (Reapproved 2009)](http://www.astm.org/Standards/E2147.htm), (incorporated by reference in §170.299) |

# 170.315(d)(3) Create and Sort Audit Report

|  |  |
| --- | --- |
| **Test Result:** | PASS:  FAIL:  No Attempt: |
| **P&S applies to all criteria:** | YES:  NO: |
| **If not, list applicable criteria:** |  |
| **Instructions:** User generates audit report for a specific time period and sorts audit log entries. | |
| **Expected Test Result:**   * Enable a user to create an audit report for a specific time period and sort audit log entries according to each of the data specified in the standards in §170.210(e) and also including:  1. Date and Time of Event; 2. Patient Identification; 3. User Identification; 4. Type of Action (additions, deletions, changes, queries, print, copy); 5. Identification of patient data that is acted upon; and 6. Changes to user privileges  * Date and time is recorded in the audit report in accordance with the standard specified at §170.210(g) Synchronized Clocks. * If applicable, the audit log report also displays actions for changes to the audit log status and/or the encryption status. | |
| **Points to Remember:**   * If also testing §170.315(d)(2), refer to Appendix C of that proctor sheet for attestation template which allows for health IT developer to attest if audit log status and/or encryption status cannot be disabled. * 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 Generate Audit Report**

|  |  |
| --- | --- |
|  | User generates audit report for a specific time period to verify the information specified below is recorded in the audit log when the health IT technology is in use:   * **Date and Time of Event** in accordance with the standard specified at §170.210(g); * **Patient Identification**; * **User Identification**; * **Type of Action** (additions, deletions, changes, queries, print, copy); * **Identification of the Patient Data that is acted upon; and** * **Changes to user privileges** |
|  | Proctor verifies date and time recorded in audit report are based on synchronized clock. |

<INSERT SCREEN SHOTS>

**1.2 Change in Audit Log Status (Conditional)**

|  |  |
| --- | --- |
|  | If changes to the audit log status are permitted by health IT module, user disables the audit log status. Otherwise, this requirement can be skipped. |
|  | User generates audit report to verify the information specified below is recorded when the audit log status is changed:   * **Date and Time of Event** in accordance with the standard specified at § 170.210(g) * **User Identification** |

<INSERT SCREEN SHOTS>

**1.3 Change in Encryption Status (Conditional)**

|  |  |
| --- | --- |
|  | If changes to the encryption status are permitted by health IT module, user disables the audit log status. Otherwise, this requirement can be skipped. |
|  | User generates audit report to verify the information specified below is recorded when the encryption status is changed:   * **Date and Time of Event** in accordance with the standard specified at § 170.210(g) * **User Identification** |

<INSERT SCREEN SHOTS>

**1.4 Sort Audit Log Entries**

|  |  |
| --- | --- |
|  | User sorts audit log information in ascending and descending order by the following data elements:   * **Date and Time of Event** in accordance with the standard specified at §170.210(g); * **Patient Identification**; * **User Identification**; * **Type of Action** (additions, deletions, changes, queries, print, copy); and * **Identification of the Patient Data that is accessed** |

<INSERT SCREEN SHOTS>

**1.5 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 “[EHR Test-128] Privacy Security Framework” provided by Drummond Group. |

<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 |  |

# 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)(3) *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 in § 170.210(e).

.

**§ 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 |
| 03-Jan-2017 | Removed ‘Changes to User Privileges’ from Sort requirement (section 1.4). |
| 01-Nov-2016 | Added test step to verify date and time in audit report utilize system clock. Added list of NIST time servers to Appendix A. |
| 01-July-2016 | Re-numbered sections. Added section 1.5 for Privacy and Security attestation. |
| 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. |
| 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