Promoting Interoperability (PI) Program Audit

Recommendations and Guidance for Eligible Hospitals & Critical Access Hospitals

This document provides information related to the audit process and guidance to assist in preparing for future audits. As noted by Centers for Medicare and Medicaid Services (CMS), all Medicare and dual-eligible(Medicare and Medicaid) hospitals participating in the Promoting Interoperability Programs may be subject to an audit by CMS and its contractor, Figliozzi and Company. States, and their contractor, will also perform audits on Medicaid providers participating in the Medicaid Promoting Interoperability Program. Letters are sent to eligible hospitals, who have received, or who are scheduled to receive, Promoting Interoperability incentive payments, requesting records related to attestation. The goal of the audit is to gather proof of the data healthcare organizations claimed when they applied for the CMS Promoting Interoperability Program. It is the customer's responsibility to maintain appropriate records and documentation in case of an audit and for providing documentation to the auditing agency.

For audit information related to Eligible Hospitals & Critical Access Hospitals for Stage 2, refer to the 6.0/6.15, Expanse, Client/Server, and MAGIC *MIS Dictionary Audit Log Guidance for PI Audit* document for MIS Dictionary setup instructions.

For audit information related to Eligible Hospitals & Critical Access Hospitals for Stage 3, refer to the audit information found in individual Best Practice documents for the measure.

MEDITECH monitors the emerging audit requirements and will notify our customers when we learn of new requirements from the audit process. At the end of this document, there is a "Lessons Learned" section based on feedback from our customers who have gone through the audit process, and a section titled "CMS Guidance Documents" which provides helpful links to CMS Audit resources.

Table of Contents

About This Guide

- This document provides Promoting Interoperability program audit recommendations and guidance for Eligible Hospitals & Critical Access Hospitals. It is the customer's responsibility to maintain appropriate records and documentation in case of an audit.
- When an edit is made to this document, the 'last updated' date in the footer will reflect this action.
- The information in this document is proprietary and should be treated accordingly.
- All images in this document are captured in a MEDITECH in-house development ring. No real patient data is used in this document, and any resemblance to live data is coincidental.
- This document is current as of the date it was downloaded/printed. To obtain an updated edition, select the appropriate document from MEDITECH's Regulatory page.
- For general questions, send an email to the Regulatory mailbox at MEDITECH, and include as much detail as you can regarding your question. For questions relating to the application setup , contact your MEDITECH Applications Specialist for the impacted product.

Audit Guidance - All Reporting Years

1. **Proof of Possession:** For proof of possession of a certified Electronic Health Record technology system, provide a copy of the Office of the National Coordinator of Health Information Technology (ONC) certification, as well as licensing agreements with the vendor(s) or invoices from the time the system was purchased.

- For proof of Certification, please visit MEDITECH's Certification page to download a copy of the Office of the National Coordinator of Health Information Technology (ONC) certification document(s). Upon request, MEDITECH will provide you with a letter regarding your licensing agreements. Requests should be submitted to your HCIS Coordinator/Account Manager for MAGIC and Client/Server, or your ARRA/PI Analyst for 6.08, 6.15, and Expanse.

2. **Core/Menu and Objective Measures:** Provide the supporting documentation, in either paper or electronic format, that was used in the completion of the Attestation Module responses (i.e. a report from your EHR system that ties to your attestation). The following are some important points:

- If you are providing a summary report from your EHR system as support for your numerators and denominators, please ensure that you can identify that the report was actually generated by your EHR (i.e. your EHR logo is displayed on the report, or step-by-step screenshots which demonstrate how the report is generated by your EHR are provided.)

- MEDITECH provides SQL report templates that enable your organization to calculate the Promoting Interoperability objective measures as defined in MEDITECH's Best Practice documentation. The reports can be printed as a summary or include patient detail. We advise our customers to print detail versions of the reports and save the output in the event of an audit. We also advise our customers to save a copy of the version of the best practice document used through the reporting period along with the best practice change log. Please visit our ARRA Best Practices web area on our Regulatory page for more information.

- For SQL reports, the MEDITECH logo cannot be presented from SQL, however the MEDITECH SQL database and tables are proprietary to our software. The suggested process is as follows:

    - Screenshot MEDITECH Data Repository Parameters routine showing the target SQL database (livedb, liveNdb, liveATdb, etc).

    - In SQL management studio, open each report and run it in the target database. Screenshot the output and ensure the target database is visible at the top of the management studio window.

- MEDITECH provides Quality Vantage for customers with 6.15 priority pack 49 and Expanse priority pack 7 and above. Quality Vantage enables your organization to calculate the Promoting Interoperability objective measures as defined in MEDITECH's Best Practice documentation. The Quality Vantage tool runs in the Live environment only.

To support Y/N attestation measures, supply documentation such as screenshots from your EHR system. Screenshots that are consistent with the CMS guidelines of settings or parameters that support the measure should satisfy the audit request.It is equally important to audit those dicationaries and parameters that have not been modified. In order to ensure your organization has a copy of how the dicationaries/parameters were set at the start and finish of your reporting period, use the dictionary or parameter list function routine.

MEDITECH also recommends generating the MIS Audit Logs regularly or using the report scheduling functionality to generate at scheduled times. It is important to note the purge parameters for the MIS Audit Logs

to ensure that printing or scheduling of reports is done before the information is purged. For additional information on report scheduling please see KB 49165 for C/S and KB 10616 for MAGIC.

Audit Guidance - 2013 and Beyond

1. Provide the documentation to support the method (Observation Services or All ED Visits) chosen to report Emergency Department (ED) admissions designating how patients admitted to the ED were included in the denominators of certain Promoting Interoperability measures (i.e. an explanation of how the ED admissions were calculated and a summary of ED admissions). A configuration parameter was created in 2013 and is used in all subsequent years to determine reporting method:

- Find **EDMethod** in the configuration table. Accepted values are: 'A' = All ED Method (POS 21 and 23) (default) and 'O' = Observation Services Method (POS 21 and Observation Patients).

- A dated screen print of this setting should be obtained.

2. **Core/Menu/Modified Objectives and Clinical Quality Measures (CQMs):** MEDITECH provides SQL report templates that enable your organization to calculate the Promoting Interoperability Objective and CQM measures as defined in MEDITECH's Best Practice documentation. The following minimum data should be saved from attestation report runs for CMS auditing:

- Compile all source code from the SQL Build Object scripts and the SQL reports that are used during attestation.
- Save audit ID's created and returned in the report output from attestation report runs.
- Create backups of all audit data tables.

The above 3 minimum data requirements are further detailed below:

- Save all ***compiled*** source code in your database from the Build Object scripts and the individual report scripts used by your organization to attest. These should be saved in a reliable location ***in accordance with your disaster recovery process*.** These scripts and objects should be available for recall in the event of audits.

  There are several ways to save the compiled code including a database backup or scripting the objects to a file in SSMS.

  Downloading and re-running current reports from Meditech.com at the time of audit is not valid as the scripts or data may have changed.

- **If using the SQL Server Management Studio:** Run the reports with the @Audit value set to 'Y' and save all audit IDs output from the report runs. An example auditID: 288F6D38-073A-43D8-B39F-F2539AC6199C

  - All of the SQL reports contain the @Audit variable within the stored procedure of the report. Setting @Audit value to 'Y' allows for an audit trail when a report is executed within the SQL database. The AuditID created for the report run is displayed in the report output. **AuditID's created from attestation runs should be saved in a reliable location in accordance with your disaster recovery process.**

  - To see these AuditIDs review the main audit table, **mtzcus_201X_XXXAuditRun or mtzcus_ModObjXX_AuditHeader** (see table below for your table name based on reporting year). The information includes the AuditID, RunTime, StartReportingPeriod, EndReportingPeriod, MeasureName, FacilityName, VendorName, VendorSoftwareVersion, AuthorName, AdmissionsMethod, EnvironmentID and the report ConfigurationParameters.

- **If using the MEDITECH Report Manager:** The AuditID's for each report are not displayed in the Report Manager output but are stored in internal tables; these tables must be accessed to obtain and save the AuditIDs.

Report Manager Version	Database	Table storing AuditIDs
1.05 and earlier	mtwebapps	**ArraWebTool_CqmReportExecutionHistoryReports**
1.06 and later	defined in your environment*	**mtzcus_ArraReportManager_JobStepParameters** (6.1 tables are in the fdb (M-AT database), 6.07 tables are in the ndb (NPR database))

* Click on your environment in the Report Manager to view your database settings.

Note: Optional information that may be of interest can be found in these additional tables:

1.05 and earlier: *ArraWebTool_CqmReportExecutionHistory*

1.06 and beyond:

- *mtzcus_ArraReportManager_Jobs*
- *mtzcus_ArraReportManager_JobCriteria*
- *mtzcus_ArraReportManager_JobStepParameters*

- **If using Quality Vantage:** When using the Quality Vantage tool, compiles used for attestation can be marked as such from the Compile tab in Quality Vantage. By changing the Attestation flag on a compile from "No" to "Yes", it will mark that compile as one that was used for attestation. Once a compile is marked as an attestation compile it cannot be deleted. When clicking the 'Date of Service Range' column for the compile you will receive a pop up box with further information. This will include the selections used in the compile and as well as the SQL AuditID that was created for this report run.

3. Back up all the audit tables with your attestation audit data and store these in a reliable location ***in accordance with your disaster recovery process*.** These tables should be available for recall in the event of audits. Audit data is stored in the following tables:

Clinical Quality Measures (CQMs)	
2013 CQM Specification Reports	**2014 CQM Specification Reports**
mtzcus_2014_eCQMAuditRun	mtzcus_2015_eCQMAuditRun
mtzcus_2014_eCQMAuditDetails	mtzcus_2015_eCQMAuditDetails
mtzcus_2014_eCQMAuditVisit	mtzcus_2015_eCQMAuditVisit
2015 CQM Specification Reports	**2016 CQM Specification Reports**
mtzcus_2015Spec_eCQMAuditRun	@SaveForAuditing value to 'Y'
mtzcus_2015Spec_eCQMAuditDetails	mtzcus_2016Spec_eCQMAuditRun
mtzcus_2015Spec_eCQMAuditVisit	mtzcus_2016Spec_eCQMAuditDetails

	mtzcus_2016Spec_eCQMAuditVisit
2017 CQM Specification Reports	**2018 CQM Specification Reports**
@SaveForAuditing value to 'Y'	@SaveForAuditing value to 'Y'
mtzcus_2018RY_eCQMAuditRun	mtzcus_2019RY_eCQMAuditRun
mtzcus_2018RY_eCQMAuditDetails	mtzcus_2019RY_eCQMAuditDetails
mtzcus_2018RY_eCQMAuditVisit	mtzcus_2019RY_eCQMAuditVisit
2019 CQM Specification Reports	
@SaveForAuditing value to 'Y'	
mtzcus_2020RY_eCQMAuditRun	
mtzcus_2020RY_eCQMAuditDetails	
mtzcus_2020RY_eCQMAuditVisit	

Core/Menu/Modified Objectives	
2014 Core Menu Reports	**2015-2016 Modified Objectives**
mtzcus_2014_CoreMenuAuditRun	mtzcus_ModObj_AuditData
mtzcus_2014_CoreMenuAuditDetails	mtzcus_ModObj_AuditDetailsOrders
mtzcus_2014_CoreMenuAuditVisit	mtzcus_ModObj_AuditDetailsPatients
	mtzcus_ModObj_AuditDetailsPrescriptions
	mtzcus_ModObj_AuditDetailsVisits
	mtzcus_ModObj_AuditHeader
	mtzcus_ModObj_AuditMeasureDetails
2017 - 2018 Stage 2	**2018-2020 Stage 3 Threshold-Based Reporting**
mtzcus_Obj2017Stage2_AuditData	mtzcus_ObjStage3_AuditData
mtzcus_Obj2017Stage2_AuditDetailsOrders	mtzcus_ObjStage3_AuditDetailsOrders
mtzcus_Obj2017Stage2_AuditDetailsPatients	mtzcus_ObjStage3_AuditDetailsPatients
mtzcus_Obj2017Stage2_AuditDetailsPrescriptions	mtzcus_ObjStage3_AuditDetailsPrescriptions

mtzcus_Obj2017Stage2_AuditDetailsVisits	mtzcus_ObjStage3_AuditDetailsVisits
mtzcus_Obj2017Stage2_AuditHeader	mtzcus_ObjStage3_AuditHeader
mtzcus_Obj2017Stage2_AuditMeasureDetails	mtzcus_ObjStage3_AuditMeasureDetails
2019 - 2020 Stage 3 Performance-Based Scoring	
mtzcus_Obj2019RY_AuditData	
mtzcus_Obj2019RY_AuditDetailsOrders	
mtzcus_Obj2019RY_AuditDetailsPatients	
mtzcus_Obj2019RY_AuditDetailsPrescriptions	
mtzcus_Obj2019RY_AuditDetailsVisits	
mtzcus_Obj2019RY_AuditHeader	
mtzcus_Obj2019RY_AuditMeasureDetails	

- The **GetAuditData** stored procedure for each set of reports can be executed to display all details of a particular audit. This stored procedure was designed to be used during a CMS audit to list the output that was produced during attestation. Save this stored procedure when saving the Build Object scripts in step 1 above.

- The **GetAuditData** procedures can be executed as follows, depending on the set of reports being run:

    - **EXECUTE mt_pr_2014_eCQMGetAuditData @AuditGUID = *'<your AuditID>'***
    - **EXECUTE mt_pr_2015_eCQMGetAuditData @AuditGUID = *'<your AuditID>'***
    - **EXECUTE mt_pr_2014_CoreMenuGetAuditData @AuditID = *'<your AuditID>'***
    - **EXECUTE mt_pr_ModObj_GetAuditData@AuditID = *'<your AuditID>'***
    - **EXECUTE mt_pr_Obj2017Stage2_GetAuditData @AuditID = *'<your AuditID>'***
    - **EXECUTE mt_pr_ObjStage3_GetAuditData @AuditID = *'<your AuditID>'***

  More information about the audit functionality can be reviewed in the **SQL Report Implementation Guide** on our Best Practice web pages.

Lessons Learned

The following information are some of the common “lessons learned” provided by customers who have gone through the audit process.

- Expect three to four rounds of requests for information from the auditors.
- Make sure your Security and Risk Analysis is performed during your reporting period, if your reporting period is a full year, or during the calendar year if the reporting period is less than a full year. The Security and Risk Analysis should be performed each year you are reporting. Complete documentation of the Security and Risk Analysis will be needed. Please read the Top 10 Myths of Security Risk Analysis from the HealthIT.gov website for common myths about Security Risk Analysis.

- The Yes/No responses will be scrutinized. Any source of various types of documentation should be kept: audit logs, screencaps of parameters and actual D/D, D/A interventions taking place (at least one) during the reporting period may help (ensure the screencaps are date stamped). An example of proving that Drug-Drug and Drug-Allergy checking took place could be accomplished by including screenshots of Pharmacy Print Orders for orders entered during the reporting period. This would demonstrate the interaction warnings that took place since the start date of the order, as well as the date the interaction check took place is included on the Pharmacy Print Order.

- Reports should be run for short time period at the beginning of your reporting period to allow for validation of data. For example, if the reporting period is one year, you should run the reports for 30, 60, 90, 180, 365 day periods (to keep track of where you are in terms of thresholds) and print/save off the copies. For a 90 day reporting period, you may want to run reports at 30, 60, and 90 days. Report and workflow validation should take place in the LIVE environment at least 30 days prior to the beginning of the reporting period.

- These 8 reports, specific to reporting in 2011-2014, have the same denominator, these should also be checked to ensure that these match:
    - Problem List
    - Medication List
    - Medication Allergy List
    - Record Demographics
    - Vital Signs, BMI, Growth Charts
    - Patient Education
    - Electronic Notes
    - Family History

  Note: For measures after 2014, there are no objectives whose denominator definitions are the same; this was confirmed by CMS.

- For any of the public health objectives please retain letters and emails from registry or public health agency confirming the receipt (or failure of receipt) of the submitted data, including: the date of the submission, name of parties involved, and whether the test was successful. Also, any dated screenshots from the EHR system that document a submission to the registry or public health agency (successful or unsuccessful) should include evidence to support that it was generated for that provider's system. For example, National Provider Identifier (NPI), CMS Certification Number (CCN), provider name, practice name, etc. From your MEDITECH EHR, this information can be taken from our interface manager and a screenshot of the message status (SENT, FAIL, etc). Further documentation could be printed through the Outbox Message report which has date/time stamp, as well as hospital/database headers to prove this was from your MEDITECH EHR.

- Print/save other information such as certification letter, screenshots, etc.

- Ensure that you have a validated and documented process for disaster recovery. Ensure that you have clean backups in case of hardware failure, etc.

- Confirm that there are at least two members of your Promoting Interoperability team that understand all of the measures, reports, validation information, selection of menu items, and information related to attestation and that the information is accessible in one place.

- Please ensure that your Promoting Interoperability contact (that was provided to CMS during your attestation process) is still currently working at your facility, as their contact information will be used for any ensuing Audit emails and letters.

CMS Guidance Documents

The following documentation details the audit requirements which are posted on the CMS website. We recommend reading each of the documents thoroughly:

- CMS Audits and Appeals Overview
- CMS Audit Overview Fact Sheet
- CMS Audit Supporting Documentation