DISTRIBUTED DATA COLLECTION (DDC) FOR REINSURANCE (RI) AND RISK ADJUSTMENT (RA): EDGE SERVER BACKUP POLICY UPDATE

January 19, 2016

Health Insurance Marketplace Program
Training Series

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Agenda

- Session Guidelines
- Intended Audience
- Purpose
- EDGE Server Backup Policy Update
- EDGE Server Data Retention Review
- EDGE Server Backup Policy
- AWS and On-Premise Specifics
- EDGE Server Restoration
- Summary
- Upcoming Webinars
- Questions
- Resources
- Closing Remarks

Session Guidelines

- This is a 90-minute webinar session.
- For questions regarding content and the DDC program, please contact your Financial Management (FM) Service Representative directly and copy the Centers for Medicare & Medicaid Services (CMS) Help Desk (CMS_FEPS@cms.hhs.gov).
- For questions regarding logistics and registration, please contact the Registrar at: (800) 257-9520.

Intended Audience

- Amazon and On-Premise External Data Gathering Environment (EDGE) server issuers (Marketplace and Non-Marketplace) of plans in states where the U.S. Department of Health & Human Services (HHS) operates the Affordable Care Act (ACA) RA and RI Programs
- Third Party Administrators (TPAs) and Support Vendors

Purpose

This presentation will:

- Review Data Retention Policy
- Provide an update on EDGE server backup policy, including requirements and best practice recommendations.

EDGE Server Backup Policy Update

EDGE Server Data Retention Review

EDGE Server Data Retention

Data Retention Policy

- Issuers must comply with the published regulatory requirements for data retention to support the Risk Adjustment and Reinsurance Premium Stabilization programs.
  - All Amazon EDGE and On-Premise EDGE server issuers are required to:
    - Retain all original data stored in their MySQL data tables for a period of 10 years.
    - Maintain their MySQL data in an active, queryable status for a period of 3 years.
      - While not required, CMS strongly recommends issuers maintain the inbound , outbound and report files on their servers for at least the entire reporting period for a coverage year for the purpose of troubleshooting and supporting submitted discrepancies and appeals.

EDGE Server Data Retention (Continued)

- CMS provided guidance on EDGE server back-up procedures on October 2, 2014 in an effort to help issuers comply with the data retention policy requirements.
- CMS is providing additional requirements and best practice recommendations to help issuers establish a regular back-up process and avoid audit findings in the event of catastrophic loss of data.

EDGE Server Backup Policy

CMS Backup Policy to Support Data Retention

- CMS is implementing additional policy guidance related to EDGE server backup to ensure data retention requirements are met by all issuers.
  - **New Requirement:** Backed up data must be moved off the server and stored in a secure location in the event of catastrophic loss.
- Issuers are required to back up their EDGE servers in accordance with the Backup Policy and User Guide for AWS and On-Premise EDGE servers starting with the 2015 data submission year.

CMS Backup Policy to Support Data Retention (Continued)

- Issuers are reminded that they are ultimately responsible for making sure the MySQL tables and files are appropriately backed up and moved off the server to a safe and accessible location.
  - Issuers should ensure any contracted parties responsible for data submission and retention have the appropriate backup procedures in place.
- CMS will not extend file submission deadlines due to a catastrophic system failure or loss of data that is irretrievable.

CMS Backup Policy to Support Data Retention (Continued)

Required Backup and Data Retention Policy:

- Issuers must move backed up final EDGE data MySQL tables to an external source after the final RA and RI calculations are run the 1st week of May.
  - Storing a backup on the EDGE server is not sufficient.
  - Backups must be moved to a secure external location other than the EDGE server in order for the data to be retrievable and accessible.
  - Storage of the EDGE data MySQL tables is the minimum requirement to meet the data retention policy.
    - Retention of inbound and outbound data files that contributed to the final calculations is a recommended best practice.

CMS Backup Policy to Support Data Retention (Continued)

Required Backup and Data Retention Policy:

- After the final RA and RI calculations are run each calendar year, CMS will require that issuers attest:
  - They have performed the backup function.
  - The backup data has been moved to an external location and
  - The data is available and accessible for future use.
- Issuers who do not comply with the backup and data retention requirements and experience a loss of data that is irretrievable may receive adverse audit findings.

Backup and Data Retention Best Practices

Best Practice Recommendations:

- CMS recommends backups be performed and data moved off:
  - After each file submission
  - After any IT upgrade or change
  - After each RA and RI calculation run
    - Backups on the EDGE server are automatically created in the **cd/opt/edge/ingest/backup** folder when this activity is executed by CMS.
- Issuer backups will help support the following critical EDGE functions:
  - Restoration activities
  - Meeting internal audit requirements
  - Supporting discrepancies and appeals that may be filed
- Issuers can find the backup command script in the EDGE Server Report Commands Job Aid posted in the REGTAP Library at https://www.REGTAP.info.

AWS and On-Premise Specifics

AWS EDGE Servers

- **Amazon EDGE servers**
  - Amazon offers options for storing MySQL tables and files outside the Simple Storage Service (S3) bucket.
  - Amazon EDGE server issuers can export and store EDGE MySQL tables and files off the AWS EDGE server to a location of their choice.
  - Issuers should not permanently store backups within the EDGE server S3 bucket.
    - Increasing Amazon S3 storage can result in deletion of existing S3 files and irretrievable loss of data.
      - Contact your FM Service Representative before attempting to increase your Amazon S3 storage.

On-Premise EDGE Servers

- **On-Premise EDGE servers**
  - Issuers are responsible for implementing their own IT backup and storage solutions.
  - Upon execution of the EDGE server backup command, issuers should verify the backup is:
    - Visible under the **cd/opt/edge/ingest/backup** folder
    - Created for all schemas with **IssuerID.SchemaName.LOCAL_BACKUP.TodayDateandTime.sql**
    - Created with the current date and time
  - Issuers should then move backup data to a secure external source.

EDGE Server Restoration

Restoring Backups

- Issuers must notify CMS immediately upon becoming aware of any issues with the MySQL tables and files, either stored or lost, which can create an access or retrieval problem.
  - Issuers should report problems as soon as possible in order for assistance to be provided before the final data submission deadline.
- To restore the backed up files, issuers must reach out to their assigned FM Service Representative at ffm.app.maint.EDGE@accenturefederal.com for coordination and instructions.
- **Amazon Web Service (AWS) issuers should not contact Amazon for assistance in restoring their files until they have been instructed to do so by CMS.**

Summary

Summary

- Issuers with either an Amazon or On-Premise EDGE server are required to:
  - Meet the regulatory requirements for data retention.
    - 10 years - Retain all original data stored in their MySQL data tables.
    - 3 years - Maintain their MySQL data in an active, queryable status.
  - Backup the MySQL data tables and move the data to an external secure location after the final EDGE server RA and RI calculations are run in May.
  - Attest that data has been moved to a secure location at the end of each benefit year.
    - Issuers are ultimately responsible for ensuring the MySQL tables and files are appropriately backed up and moved off the server to a safe and accessible location.

Summary (Continued)

- CMS' best practice recommendations for all issuers:
  - Back up and move data off the server frequently to support restoration activities, internal audit requirements and discrepancies and appeals that may be filed.
- Issuers must notify CMS via their FM Service Representatives at (ffm.app.maint.EDGE@accenturefederal.com) or the CMS Help Desk (CMS_FEPS@cms.hhs.gov) , immediately upon becoming aware of:
  - An actual or potential loss of data
  - A need to perform recovery activities or,
  - A need to increase the Amazon EDGE server memory.

Summary (Continued)

- Issuers can access helpful documents in the REGTAP Library including:
  - The backup command script in the EDGE Server Report Commands Job Aid.
  - Backup Policy and User Guide for AWS and On-Premise EDGE Servers.

Upcoming Webinars

HTTPS://WWW.REGTAP.INFO/

Upcoming Webinars

Webinar Topic	Scheduled Event Date
February 26, 2016 EDGE Server Maintenance Release	January 26, 2016 11:30 a.m. – 1:00 p.m. ET

Questions?

To submit questions by phone:

- ❑ Dial ‘14’ on your phone’s keypad.
- ❑ Dial ‘13’ to exit the phone queue.

HTTPS://WWW.REGTAP.INFO/

Resources

HTTPS://WWW.REGTAP.INFO/

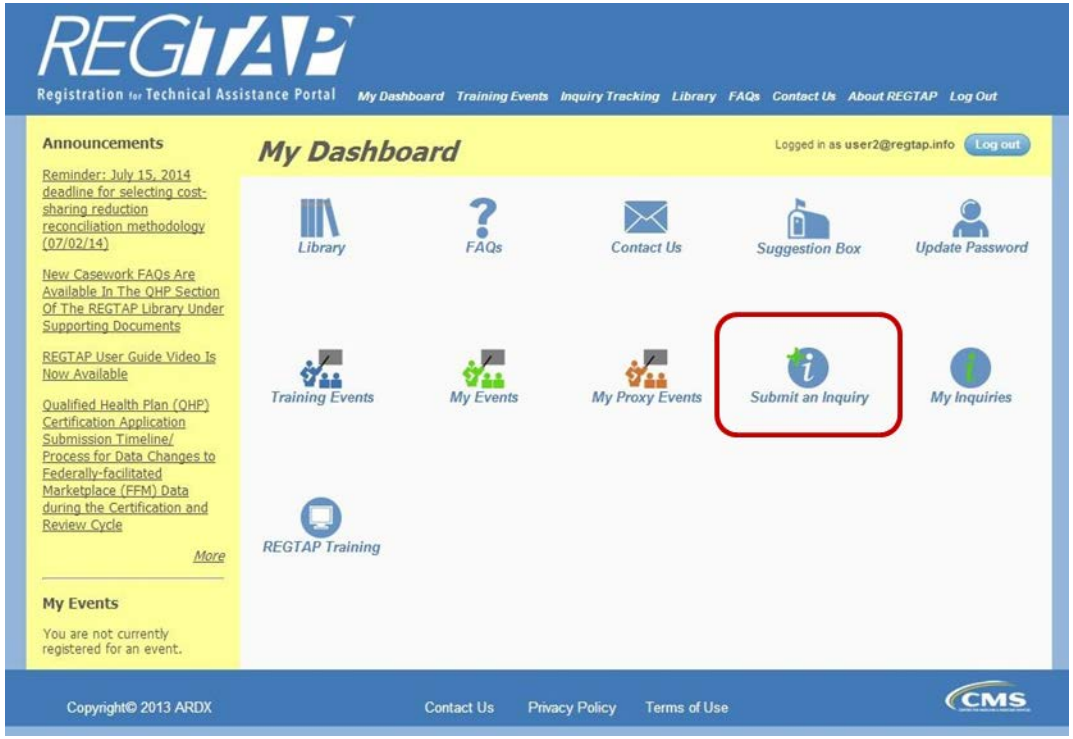
Resources

Resource	Link/Contact Information
Center for Consumer Information and Insurance Oversight (CCIIO)	http://cms.gov/cciio/
Registration for Technical Assistance Portal (REGTAP) • Registration • Inquiry Tracking and Management System (ITMS) • Resource Library • Frequently Asked Questions (FAQs)	https://www.REGTAP.info/

Inquiry Tracking and Management System (ITMS)

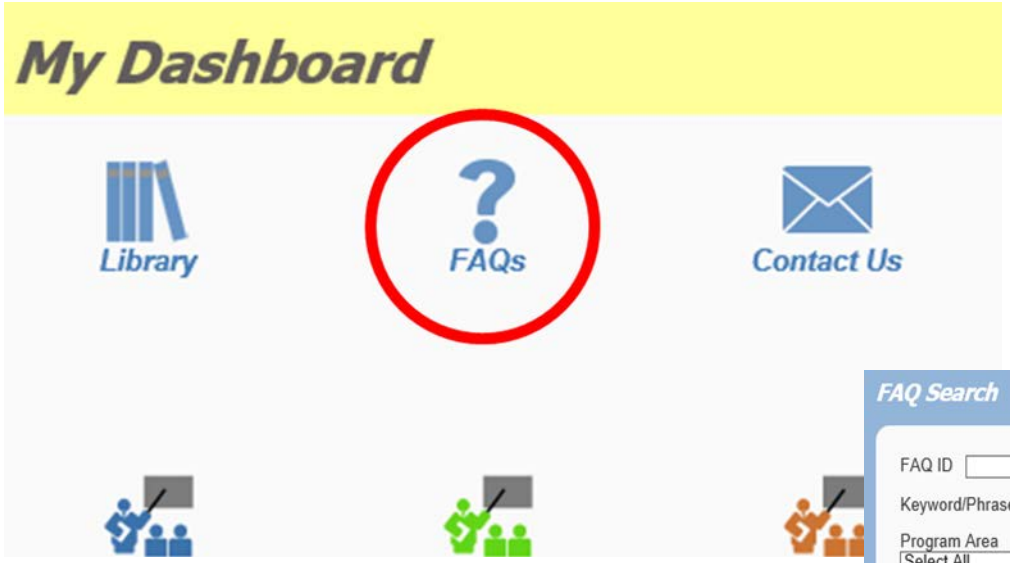
ITMS is available at https://www.regtap.info/

Users can submit questions after the Webinar by selecting "Submit an Inquiry" from My Dashboard.



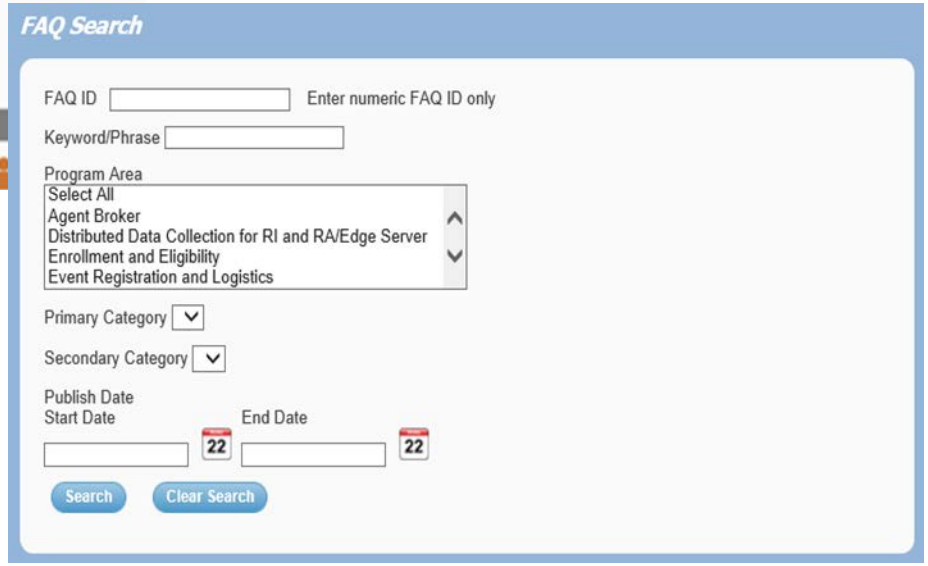
Note: Enter only one (1) question per submission.

FAQ Database on REGTAP



The FAQ Database allows users to search FAQs by FAQ ID, Keyword/Phrase, Program Area, Primary and Secondary categories, and Publish Date.

FAQ Database is available at https://www.regtap.info



Closing Remarks

HTTPS://WWW.REGTAP.INFO/