Overview of Qualified Health Plan (QHP) Issuer Compliance in the Federally-Facilitated Exchanges (FFE)

April 29, 2020

Qualified Health Plan (QHP) Issuer Conference

The information provided in this presentation is not intended to take the place of the statutes, regulations, and formal policy guidance that it is based upon. This presentation summarizes current policy and operations as of the date it was shared. Links to certain source documents may have been provided for your reference. We encourage persons attending the presentation to refer to the applicable statutes, regulations, and other guidance for complete and current information.

HTTPS://WWW.REGTAP.INFO

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Agenda

- FFE Compliance Reviews - Overview
- Compliance Reviews
- Post-Certification Assessment (PCA)
- Machine Readable
- Renewal and Discontinuance Notices
- Privacy & Security
- Questions

FFE Compliance Reviews—Overview

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

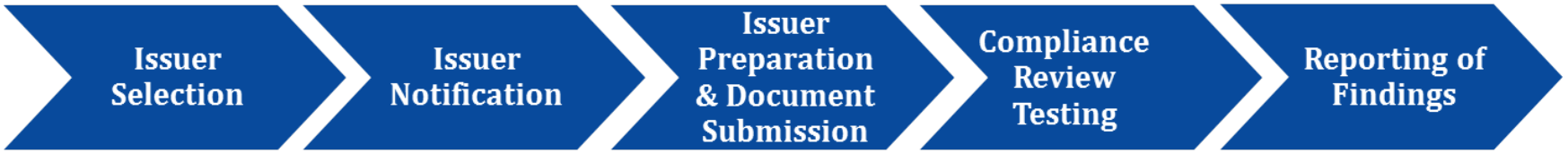
HTTPS://WWW.REGTAP.INFO

FFE Compliance Reviews: Legal Scope

- Applies to all issuers operating in an FFE.
- Compliance with FFE-specific requirements.
  - Mostly 45 CFR Part 156.

FFE Compliance Reviews: Timing

- A general overview of the FFE compliance review process is shown below:



- 3 groups of selection notices to issuers
- Sent between March and October

FFE Compliance Reviews: Limits

- FFE compliance reviews are not the same checks as:
  - QHP certification,
  - Advanced Premium Tax Credit (APTC) audits,
  - Medical Loss Ratio (MLR) audits, or
  - Any other audit program operating in CCIIO.
- Compliance reviews focus on FFE-specific standards and processes.

2019 FFE Compliance Reviews: A Snapshot of Past Reviews

- CMS selected 22 Issuer IDs for the 2019 FFE compliance reviews.
- This represented 17 states.
- CMS conducted both desk and onsite compliance reviews.
- Reviews focused on specific areas of issuers' participation and activities in the FFE.
- Reference: Key Priorities for FFE Compliance Reviews for the 2019 Plan Year.
  - https://www.cms.gov/CCIIO/Resources/Forms-Reports-and-Other-Resources/Downloads/Key-Priorities-FFM-2019.pdf

2019 FFE Compliance Reviews: A Snapshot of Past Reviews (continued)

- Similar to 2018, the 2019 FFE compliance reviews focused on reviewing a combination of issuers' policies and procedures and testing issuers' processes related to FFE operations. For example:
  - Policies on ensuring online provider directories are up-to-date and providing hard copy provider directories upon request (45 CFR 156.230(b)).
  - Operational process for reviewing and resolving consumer complaints forwarded to QHPs and QHP issuers in FFEs (45 CFR 156.1010).

2019 Compliance Reviews: Lessons Learned

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

HTTPS://WWW.REGTAP.INFO

2019 Compliance Reviews: Lessons Learned

- Issuers that use a provider network were required to contract with at least 20% of Essential Community Providers (ECPs) in their plans' service areas, make contract offers in good faith to at least one ECP provider in each specific ECP category in each county (where available), and make a contract offer in good faith to every Indian health provider in their plans' service areas (45 CFR 156.235(a)).

- **Observations:** Some issuers did not keep appropriate records of good faith contract offers to ECPs sufficient for testing. Even if the provider refuses the contract offer every year, you must issue the contract offer and retain a record of that offer. You do not need proof of a response.

2018 Compliance Reviews: Lessons Learned (continued)

- Required language in delegated and downstream entity agreements (45 CFR 156.340(b)).
  - Specify activities, reporting, and remedies for breach as determined by either the issuer or HHS.
  - Specify that entity must comply with all applicable laws and regulations. Best practice is to cite specific legal provisions to put entity on notice and follow with a blanket statement to cover future changes in laws and regulations.
  - Specific clauses requiring entity to permit access to HHS in connection with audits or inspections of the entity's records related to the delegated functions.
- **Observations:** CMS has found agreements lacking the specific required language in many reviews. Language is required for both existing and new agreements.

2018 Compliance Reviews: Lessons Learned (continued)

- Privacy Breach and Incident Reporting Requirements (QHP Agreement).
  - Per the QHP Agreement, issuers must report any breach or potential breach of Exchange data within **24 hours** to the CMS IT Service Desk (cms_it_service_desk@cms.hhs.gov).
  - For privacy incidents, the QHP Agreement requires reporting within **72 hours**.
- **Observations:** Many issuers assume that reporting requirements for Exchange breaches don't require any deviation from Health Insurance Portability & Accountability Act (HIPAA) reporting requirements. Exchange reporting requirements are *distinct from, and in addition to,* similar requirements pursuant to HIPAA.

2018 Compliance Reviews: Lessons Learned (continued)

- Provider Directory Inaccuracies (45 CFR 156.230(b)(2)).
  - A QHP issuer must publish an up-to-date, accurate, and complete provider directory including information on which providers are accepting new patients, the provider's location, contact information, specialty, medical group, and any institutional affiliations…
- **Observations:** Issuers who had the lowest rate of errors in their provider directories:
  - Performed regular (e.g. monthly) outreach to their provider networks to update directory information,
  - Included the office or practice name alongside the identifying information for the individual provider (e.g. John Smith, DDS works at BrightSmile Dentistry), and
  - Allowed users to search providers by QHP or product names rather than network name.

Compliance Reviews in 2020

More Information

- 2018 Summary Compliance Review Report
  - Found at: https://www.cms.gov/CCIIO/Resources/Forms-Reports-and-Other-Resources/Downloads/2018-PY-FFE-Summary.pdf
  - Useful information on review methods and common findings!

Post-Certification Assessment (PCA)

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

HTTPS://WWW.REGTAP.INFO

Post-Certification Assessment (PCA)

- PCA is an annual process that flags potential concerns with issuer data
- PCA generally occurs soon after certification of Qualified Health Plans (QHPs)
- PCA flags potential issues that are likely to affect consumers prior to the beginning of the plan year

PCA (continued)

- For Plan Year (PY) 2020, PCA reviews focused on several topics, including:
  - Provider Directories
  - Formularies
  - Benefits
- Issuers flagged for potential issues were notified by CMS in November 2019, with resolutions due in January 2020
- There was an increase in the number of unresolved issues by the deadline this year.

PCA (continued)

Observations in PY 2020 PCA reviews:

- Most concerns related to Benefits in the following categories:
  - Nonfunctional URLs or URLs that did not lead to where they are required
  - Information in the Summary of Benefits and Coverage (SBC) did not match the Plans and Benefits Template (PB&T)

PCA (continued)

- Most common concerns in the URL reviews (Provider Directory, Formulary, Benefits):
  - URL Inaccessible – meaning it did not work, went to an “Under Construction” page, or the directory or formulary, etc. could not be found using the submitted URL
  - Difficult to Access – page could eventually be found, but was either hidden from plain view or the reviewer determined that a consumer would not reasonably be able to determine where the page was located

Machine Readable (MR)

Machine Readable (MR) Requirements

- Issuers are required to publish provider and formulary data on websites
  - Must be in a machine readable (MR) format as specified by HHS - HHS specifies JavaScript Object Notation (JSON) format
  - **Index URL's need to be submitted by June 17th, 2020**
  - **New PY data needs to be ready by Aug 19th, 2020**
  - Must update MR information at least once monthly

MR Compliance Activities

- CMS monitors compliance with the MR requirements:
  - Pre-Open Enrollment (OE) review starting in July 2020 to track readiness
  - Track compliance during compliance reviews
  - Post-OE review of issuer websites against current issuer-submitted-MR files

MR Compliance (continued)

- Common issues – uncrawlable, not updated, missing required fields, invalid National Provider Identifiers (NPIs)

- Resolution of MR Compliance Issues
  - Technical Assistance
  - Notice of Non-Compliance

- Issuer can ask MR questions in the UserVoice platform
  - https://cms-provider-directory.uservoice.com/
  - Also contains Knowledge Base documents

Renewal and Discontinuance Notices (R&D)

Renewal and Discontinuance Notice Purpose

- Review of notices sent to consumers in the previous Calendar Year for the current Plan Year
- Issuers must:
  - Include certain information in renewal and discontinuation notices to their enrollees
  - Send notices in a form and manner specified by CMS in the September 2, 2016 and July 19, 2018 bulletins
- CMS reviews renewal and discontinuation notices to ensure compliance with 45 CFR 147.106 and 45 CFR 156.1255

Renewal and Discontinuance Notice Review Scope

CMS reviews the renewal and discontinuation notices for compliance with applicable requirements and guidance in five areas:

- **Notice Format and Content:** Did the notice comply with content and formatting requirements?
- **Timeliness:** Was the notice delivered to enrollees before the first day of the Open Enrollment Period (OEP)?
- **Notice Recipient:** Was the recipient identified on the Renewal or Discontinuance Notice consistent with the information included with supporting documentation and attachments.

Renewal and Discontinuance Notices (Continued)

- **Deductible and Maximum Out-of-Pocket (MOOP):** When a significant change in deductibles and MOOPs was indicated, were the changes communicated to enrollees in the notice or via reference to supplemental materials, such as the Summary of Benefits and Coverage (SBC)?

- **Benefit Value Changes:** Were significant benefit-level changes called out directly in the notice or by reference to supplemental materials?

Privacy & Security

What's Required of QHP Issuers?

- The Privacy & Security Agreement between QHP issuers and CMS requires issuers to report, by phone or email, to CMS IT service desk:
  - *Any* suspected (when a potential breach to Personally Identifiable Information (PII) has occurred) or confirmed breaches of personally identifiable information (PII) within 24 hours from knowledge of the breach.
  - Suspected or confirmed security Incidents within 72 hours of discovery of the incident.
  - In the event of an Incident or Breach, QHPIs must permit CMS to gather all information necessary to conduct all Incident or Breach response activities deemed necessary by CMS
- **Note that these reporting requirements are distinct from, and in addition to, similar requirements pursuant to the Health Insurance Portability & Accountability Act (HIPAA).**
- The Agreement defines PII, breach, and incident based on OMB guidance.

OMB Privacy & Security Guidance

In accordance with OMB Memorandum (M) 07-16 "Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)", CMS has implemented a process for protecting (PII) and created policy requirements for partners to notify the proper authorities in the event that an incident, breach, or potential breach, to PII has occurred.

- PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, legal permanent resident, or a visitor to the U.S.

- PII may include, but is not limited to, data elements such as: names, addresses, dates of birth, Social Security numbers, and medical history.
  - Can the information be used to identify an individual, independently, or when linked with other information?
  - Information that is not PII can become PII when linked with other information - from any source - that would make it possible to identify an individual.

OMB Privacy & Security Guidance

- A breach is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. (Defined in OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information").
- Some other common examples of breaches include:
  - A laptop or portable storage device storing PII is lost or stolen;
  - An email or letter containing PII is inadvertently sent to the wrong person; and
  - An authorized user accesses or uses PII for an other-than-authorized purpose.

- An incident is a adverse event or action that is unplanned, unusual, and unwanted that happened as a result of non-compliance with the privacy policies and procedures of the Department. It must pertain to the unauthorized use or disclosure of PII including "accidental disclosure" such as misdirected e-mails or faxes.

More Information

- **FAQ:** Reminders to Qualified Health Plan Issuers: CMS QHP Agreement Requirements for Personally Identifiable Information Breach and Security Incident Reporting.
- **Found at:** https://www.cms.gov/CCIIO/Resources/Fact-Sheets-and-FAQs/Downloads/ReminderQHPAgreement.pdf
- **FAQ:** Web-broker Personally Identifiable Information (PII) incident and breach reporting requirements.
- Found at: https://zone.cms.gov/document/web-broker-guidance-and-frequently-asked-question-faq-documents

Questions?

- To Submit or Withdraw Questions by Phone:
  - *If you are listening through your computer speakers and want to submit a question by phone, dial* 1-866-391-5945 and enter your unique six-digit PIN, then dial *"star(*) pound(#)" on your phone's keypad.*
  - *If you are already dialed in by phone and want to submit a question, then dial "star(*) pound(#)" on your phone's keypad.*
  - *If you would like to withdraw a question and you are dialed in by phone, then dial "star(*) pound(#)" on your phone's keypad.*
- To submit questions by webinar:
  - *Type your question in the text box under the "Q&A" tab and click "Send."*