Phase 2 Data Security Audit Requirements

The Phase 2 Data Security Audit is a review of requested information that validates compliance with required CMS Acceptable Risk Safeguards (ARS) security controls. Entities provide documentation to address the following questions:

- Describe the private sources of other data that you will combine with CMS data.
- Describe where the de-identification, aggregation, storage, and processing of data occurs.
- Describe any additional vendors/partners that assist in developing measures or other analyses.
- Describe how the lead entity receives the identified or de-identified provider analyses and reports.
- Describe how the lead entity finalizes the Phase 3 submission for CMS approval.
    - Note: This evidence submission and approval process is only required once prior to the QEs first round of public reporting. Prior to additional rounds of public reporting, the QE communicates changes to measures and reports via the QECP ongoing program administration reported changes process.
- Describe how the lead entity distributes confidential reports to practices and/or providers for corrections and appeals.
    - Note: This step is only necessary if the lead entity plans to report on data at the provider level.
- Describe how the lead entity completes the corrections and appeals process.
- Describe how the practices and/or providers review reports and make corrections.
- Describe how the lead entity distributes final approved reports to the public.