Centers for Medicare & Medicaid Services

U.S. Department of Health and Human Services

Streamlined Modular Certification for Medicaid Enterprise Systems Certification Guidance

Version 1.0

April 2022

Table of Contents

EXECUTIVE SUMMARY

As mentioned in the State Medicaid Directors Letter (SMDL), ***"Streamlined Modular Certification for Medicaid Enterprise Systems,"*** (hereafter referred to as "the SMDL"), the Centers for Medicare & Medicaid Services (CMS) continues to streamline the certification approach and move towards Outcomes-Based Certification (OBC) for Medicaid Enterprise Systems (MES) Information Technology (IT) projects. The SMDL introduced a significantly Streamlined Modular Certification process and formally sunsets the existing processes known as the Medicaid Enterprise Certification Toolkit (MECT) and the Medicaid Eligibility and Enrollment Toolkit (MEET).

For all MES IT projects going forward, states should follow the guidance for the Streamlined Modular Certification process in the SMDL as well as this "Streamlined Modular Certification for Medicaid Enterprise Systems Guidance" (Certification Guidance) document. States should not use MECT and MEET for MES IT projects initiated after the publication of the SMDL and this Certification Guidance.

This Certification Guidance, which builds upon elements outlined in the SMDL, consists of an overview document along with multiple appendices, all providing more specificity around Streamlined Modular Certification (i.e., outcomes, basic indicators of project health, metrics, and operational reports). In addition, this Certification Guidance details how Milestone Reviews will differ substantially from those required under the MECT and MEET.

Finally, in line with the effort to reduce state burden and move towards an OBC approach, CMS is implementing the following changes:

- Reducing the number of required, state-submitted MES review artifacts from 29 to seven.
- States are no longer required to submit a Project Partnership Understanding (PPU) or Independent Verification & Validation (IV&V) Quarterly Certification Progress Reports.
- CMS will accept an alternative format for the MITA State Self-Assessment (SS-A), if preferred.

ABOUT STREAMLINED MODULAR CERTIFICATION

CMS has been working with states to test and refine proposed processes and tools aimed at defining and implementing a new OBC method.[1] CMS views Streamlined Modular Certification as the next interim step in that learning process and one that will promote effective stewardship of federal funding well into the future.

With the goal of delivering consistency and accountability for CMS's certification processes, the SMDL established a unified certification process for all MES, a term synonymous with mechanized claims processing and information retrieval system (MCPIRS) as defined at 42 C.F.R. §433.111(b). The term MES represents a system composed of the sum total of Medicaid IT systems that are used by the Medicaid agency to manage, monitor, and administer the state's Medicaid program. The MES is composed of modules that support a state's Medicaid operations and include those described in ***Appendix B, CMS-required outcomes for specific MES modules***, among other functions and modules.

[1] *CMCS Informational Bulletin*, "Outcomes-based Certification for Electronic Visit Verification (EVV) Systems," October 24, 2019. https://www.medicaid.gov/sites/default/files/Federal-Policy-Guidance/Downloads/cib102419.pdf.

For all systems that comprise the MES, the Streamlined Modular Certification approach is designed to:

- Demonstrate measurable improvements to a state's Medicaid program resulting from the delivery of a new module or enhancement to an existing system.
- Leverage data and testing to inform our assessment of the successful delivery of systems and inform subsequent funding decisions.
- Enable operational reporting for system performance and functionality to ensure ongoing oversight of data and evidence that demonstrates the continuous achievement of required and desired outcomes.
- Reduce burden on states and CMS during the certification process without compromising CMS's responsibility to ensure those systems satisfy all statutory and regulatory requirements.
- Advance incrementally toward a fully realized OBC process for the entirety of MES.

An important principle of Streamlined Modular Certification is to reduce burden on states and CMS during the certification process without compromising CMS's responsibility to ensure those systems satisfy all statutory and regulatory requirements. Based on lessons learned from the MECT and MEET reviews and feedback from states, CMS is reducing the number of required state-submitted MES review artifacts from 29 to seven. Please see ***Appendix C: Required Artifacts List,*** for additional information regarding each of the required artifacts.

ELEMENTS FOR STREAMLINED MODULAR CERTIFICATION: CONDITIONS FOR ENHANCED FUNDING, OUTCOMES, AND METRICS

The Streamlined Modular Certification process for MES is structured around three elements:

- **Conditions for Enhanced Funding –** As a condition of receiving enhanced federal matching funds for state expenditures on MES as described above, states must ensure that the system complies with all of the conditions for enhanced funding as provided in 42 C.F.R. §433.112 and that the system remains compliant with federal Medicaid requirements for enhanced operations matching once it is in operation as provided in 42 C.F.R. §433.116. Please see ***Appendix A: Conditions for Enhanced Funding.***

- **Outcomes –** Outcomes describe the measurable improvements to a state's Medicaid program that should result from the delivery of a new module or enhancement to an existing system. Outcomes should support Medicaid program priorities, be directly enabled by the state's IT project, and be stated in the Advance Planning Document (APD). If a project has an already-approved APD that does not include applicable outcomes, CMS will work closely with the state to identify and validate project outcomes as part of the APD-Update (APD-U) process or during preparation for a review. CMS is encouraging states to develop measurable, achievable outcomes that reflect the MES project's short-term goals.

  CMS-required outcomes are based on statutory or regulatory requirements and provide a baseline for what is required of an MES, including the efficient, economical, and effective administration of the state's Medicaid program. They are generally associated with the module(s) the project is trying to put in place or improve. Please see ***Appendix B: CMS-***

Required Outcomes for Specific MES Modules for the CMS-required outcomes expected for each module.

State-specific outcomes reflect the unique circumstances or characteristics of the state or territory and its Medicaid program and focuses on improvements to the program not specifically addressed by the CMS-required outcomes. For example, a state may request funding to implement functionality that will increase the number of no-touch eligibility determinations or improve the quality of encounter data to conduct more effective oversight of managed care entities. States that are requesting enhanced Federal Financial Participation (FFP) for systems that fulfill business needs beyond minimum legal requirements should work with their CMS State Officer to finalize outcomes that address the proposed functionality. Additionally, state-specific outcomes may reflect the unique circumstances or characteristics of the state or territory and its Medicaid program.

CMS anticipates that states may need to revisit and update outcomes and metrics (as defined below) for their investment over time. This may be a result of lessons learned as part of a continuous improvement assessment or changing Medicaid priorities (reflecting changes made by the state or CMS). By doing so, the state maintains alignment to current needs for programmatic value within its IT investments. Any revisions to a state's CMS-required or state-specific outcomes or metrics require submitting an APD-Update (APD-U). The state should regularly contact their CMS State Officer to discuss such updates.

- **Metrics –** Metrics provide evidence that the outcomes are met on an ongoing basis. In accordance with 42 C.F.R. §433.112(b)(15) and §433.116(b), (c), and (i), states must be capable of producing data, reports, and performance information from and about their MES modules to facilitate evaluation, continuous improvement in business operations, and transparency and accountability, as a condition for receiving enhanced federal matching for MES expenditures. Metrics reporting enhances transparency and accountability of IT solutions to help ensure the MES and its modules are meeting statutory and regulatory requirements as well as the state's program goals. State reporting also gives states and CMS early and ongoing insight into program evaluation and opportunities for continuous improvement. Examples of metrics for MES modules can be found on the CMS Certification GitHub Repository, which can be accessed at **https://cmsgov.github.io/CMCS-DSG-DSS-Certification/**.

To illustrate CMS-required and state-specific outcomes and metrics, consider the following hypothetical example:

Example of Outcomes and Metrics to Achieve a State Program Goal

State program goal: Reduce the average amount of time it takes to process Medicaid applications. To help achieve this goal, the state wants to begin a project to maximize real-time Modified Adjusted Gross Income (MAGI)-based eligibility determinations.

State-specific outcomes:

- Increase the percentage of real-time MAGI-based eligibility determinations conducted
- Increase the percentage of applications submitted online

CMS-required outcomes:

- The eligibility system receives, ingests, and processes the single-streamlined applications, change of circumstances, renewal forms, and any supporting documentation requested by the state (including telephonic signatures) from individuals, for all Medicaid eligibility groups and CHIP through online via multiple browsers (EE1).
- The eligibility system uses automated interfaces with electronic data sources to enable real-time or near real-time, no manual touch eligibility determinations (EE5).

Metrics:

- Average time to conduct a MAGI-based eligibility determination
- Percentage of Medicaid applications submitted via online application
- User satisfaction, as measured by surveys

REQUIRED EVIDENCE

States will be required to provide the following data, reports, and performance information, pursuant to 42 C.F.R. §433.112(b)(15) and §433.116(b), (c), and (i), as applicable. This documentation will help demonstrate whether conditions for enhanced funding are met, intended outcomes are being achieved, and metrics are being successfully collected and reported.

- Evidence to support outcome achievement may include, but is not limited to:
  - Demonstrations
  - Testing results
  - Production reports
  - Plans for organizational change management (e.g., managing stakeholders and users, training, help desk)

  States should provide the evidence they use to determine their module is production-ready (that is, ready to be put into operation) which could include test results and other data illustrating the module's capability of achieving intended outcomes. States should also

demonstrate that their operations staff are implementation-ready (e.g., documentation of trainings and other relevant organizational change management activities that have been conducted and/or are ongoing) to support the successful delivery of the module and ongoing operations. In addition, once the module is in operations, states should provide the evidence that they continue to comply with applicable regulations and meet programmatic outcomes.

- Evidence from the metrics that are collected and reported will be evaluated to determine whether the system is achieving the identified outcomes. As required by 42 C.F.R. §433.112(b)(15) and §433.116(b), (c), and (i), throughout the IT investment lifecycle, states will continue reporting on metrics to ensure that solutions meet regulatory requirements and are measurably supporting desired program outcomes. CMS State Officers will collaborate with states to conduct reviews and assessments based on metric reports, helping to ensure continued success and improvement of MES solutions. CMS will coordinate with states to use existing data sources and reporting systems, such as Transformed Medicaid Statistical Information System (T-MSIS) and Medicaid and CHIP Performance Indicators, to avoid redundancy and minimize administrative burden whenever possible.

In addition, CMS has found that properly tested systems and, in particular, those tested by actual users throughout the entire development process, have a better chance of successful implementation. Therefore, CMS is putting an emphasis on testing in the certification process. The ***Testing Guidance Framework*** document accompanying this SMDL offers specific MES testing expectations and recommendations. CMS plans to release additional materials describing updated software development best practices in the future, which CMS anticipates states will incorporate into their future MES development efforts.

INFORMATION TECHNOLOGY INVESTMENT LIFECYCLE ENGAGEMENT AND CERTIFICATION PROCESS

Streamlining the modular certification process depends on an engagement model that a) relies on a close, ongoing partnership between CMS and the state throughout the IT investment lifecycle, and b) involves regular discussions and check-ins on state progress toward achieving shared goals for the project. In piloting this model for Electronic Visit Verification (EVV) system certification, both states and CMS found tremendous value in ongoing collaboration. CMS will continue working with states to enhance the ongoing partnership model on which OBC depends. States should regularly engage with their CMS State Officers throughout the IT investment lifecycle, especially as states begin to plan their IT investments.

As shown in Figure 1, engagement during each phase of the IT investment lifecycle might include the following touchpoints:

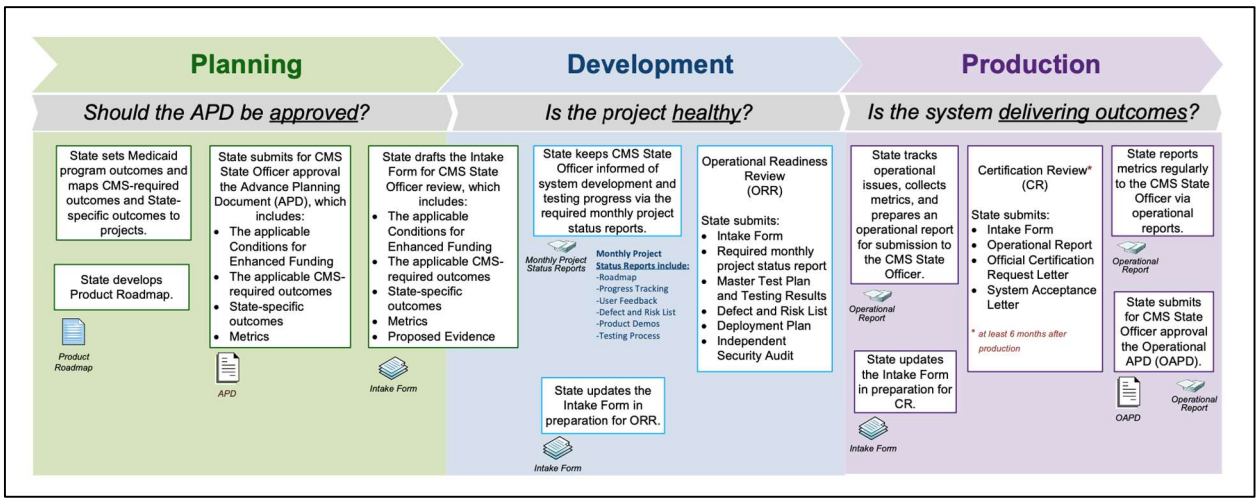

Figure 1. Streamlined Modular Certification Process Timeline

THE STREAMLINED MODULAR CERTIFICATION PROCESS

As articulated in the *Figure 1. Streamlined Modular Certification Process Timeline* visual and discussed above, the certification model for states is changing in a fundamental way – **away from checklists, and towards regular conversations between states and CMS on what a state is trying to achieve with any given investment.**

PROJECT PLANNING PHASE

With Streamlined Modular Certification, there is a strong emphasis on early, frequent conversations and collaboration between states and CMS. Before an APD is written, the state should draft their planned program outcomes and map outcomes to projects. The state should then articulate their planned CMS-required and state-specific outcomes, metrics, and how they propose to demonstrate achievement of those results. Next, the state should:

- Articulate a planned product roadmap (aligned to an overall state MES roadmap)
- Draft and review the APD with their CMS State Officer
- Submit the APD for official CMS review and approval

CMS expects the APD/APD-U to describe the programmatic value, aligned to state priorities, that a state plans to achieve with their project. The APD/APD-U should include measurable outcomes and metrics that align with the desired Medicaid program goal(s). States should be in frequent contact with their CMS State Officer during the planning process. This provides the state with CMS support with the development of APDs that reference the applicable Conditions for Enhanced Funding, and include outcomes and metrics that clearly align the proposed IT project with the state's goals, whether it be to solve a problem or achieve improvements to the Medicaid program.

If a state has an approved project APD that does not include applicable outcomes, CMS will work closely with the state to identify and validate outcomes for that project as part of the APD-U process or during preparation for a review.

PROCUREMENT PLANNING PHASE

After the APD is approved, the state then moves into procurement planning. States can consult with their CMS State Officer to help ensure the state's outcomes are articulated to prospective vendors. Prior to releasing an RFP, the state should document the approved CMS-required outcomes, state-specific outcomes, and metrics in the ***Streamlined Modular Certification Intake Form Template*** for discussion and approval with their CMS State Officer. Together, they should agree on a preliminary list of evidence that will be used to demonstrate that outcomes have been achieved. These outcomes and metrics (and associated evidence) will be assessed at the Operational Readiness Review (ORR) and Certification Review (CR).

DEVELOPMENT PHASE

At the beginning of the Development phase, the state should develop a Master Test Plan, in consultation with the ***Testing Guidance Framework*** when starting system development. The state should provide their CMS State Officer regular development and testing progress in the form of testing results, defect reports, and regular software demonstrations. The state should also keep their CMS State Officer apprised of progress toward achieving the Conditions for Enhanced Funding and desired program outcomes.

As described in more detail below, CMS is no longer requiring states to submit the PPU or IV&V Quarterly Certification Progress Reports. Instead, states should use the required monthly project status reports during the Development phase (required as part of APD/APD-U approval) to submit information showing the state 's IT projects aligns with Streamlined Modular Certification and appropriately demonstrates project health. The monthly project status should be submitted to their CMS State Officer, and either the MES mailbox (MES@cms.hhs.gov) or CMS Box.

Demonstration of project health should focus on the following areas:

- ***Achieving targets and milestones:*** The state should identify how their team will measure incremental progress toward intended outcomes throughout the Development phase and regularly after production (including incremental releases and/or pilots of new functionality). The state must describe, in a timeline or roadmap, how the state will achieve and implement functionality, including priorities, dependencies, and milestones. These artifacts are expected to evolve as the state gains information during development, and necessary adjustments will be discussed during regular check-ins with their CMS State Officer.

- ***Use of testing to ensure functionality is being delivered:*** State testing should be informed by the ***Testing Guidance Framework*** document, which offers specific MES testing expectations and recommendations. As mentioned above, the state should develop a master test plan that describes the details for how and what testing will occur and provide test results throughout the Development phase and leading up to the ORR. The state should emphasize user engagement during the testing process and include actual users in both user acceptance and usability testing. Furthermore, the test results should not only validate the iterative delivery of system functionality, but also confirm that the system will produce metrics associated with approved outcomes.

- **Monthly project status reports should include the following:**

    - ***Roadmap*** – An up-to-date product roadmap identifying current, planned, and future functionality and milestones
    - ***Progress Tracking*** – A regular report measuring development progress and progress towards achieving outcomes
    - ***User Feedback*** – A report showing how user feedback is regularly incorporated into development
    - ***Defect and Risk List*** – Known defects and risks that may cause delays and any mitigations or workarounds
    - ***Product Demos*** – Demo of functionality/features, or regular report of code/feature releases
    - ***Testing Process*** – A documented testing process aligned with the CMS ***Testing Guidance Framework***

CMS will continue to provide comprehensive technical assistance to states during the Development phase of their IT investment lifecycle.

PRE-PRODUCTION PHASE: OPERATIONAL READINESS REVIEW

The state must undergo an ORR with their CMS State Officer prior to releasing their system/module into production. The state should schedule the ORR with their CMS State Officer well in advance of the state's planned go-live date and together define the scope of the review. The state will need to demonstrate – with appropriate evidence – that the system is ready to be released, that it is likely to achieve the approved CMS-required and state-specific outcomes, and it can support the generation and reporting of metrics that were approved in the APD.

If a state is taking a phased approach to implementation, the state and their CMS State Officer will decide the most appropriate point in which to conduct the ORR. The ORR date should be scheduled to provide sufficient time to prepare for the review (approximately six months). During the ORR preparation period, CMS and the state should determine the minimum set of Required Artifacts (listed in ***Appendix C: Required Artifacts List***) and evidence needed to demonstrate the project is ready to enter production and that outcomes are likely to be achieved. Evidence includes the required Independent Security Audit, which is discussed in more detail in ***Appendix D: Framework for the Independent Third-Party Security and Privacy Assessment Guidelines for Medicaid Enterprise Systems***. Any required legal non-disclosure and data-sharing agreements should be prepared for the review of the relevant module.

CMS strongly believes that proper and complete systems testing, particularly testing with users, is an important indicator of project success. Hence, testing results are a core part of what will be evaluated during ORR. The evidence (e.g., testing results, demonstrations, plans for organizational change management) must clearly demonstrate that:

- The required Conditions for Enhanced Funding applicable to that project and described in the APD/APD-U are met.
- The IT functionality associated with the applicable CMS-required and state-specific outcomes and described in the APD/APD-U has been developed and tested in accordance with the state's master test plan.
- The system will support the collection and reporting of metrics described in the APD/APD-U.

CMS has found that tailoring materials and reviews based on what the state is trying to accomplish through a given investment is more effective and meaningful for both states and CMS. Therefore, an Intake Form will be customized for the state's ORR. For the ORR, the following steps are completed:

1. The state completes the state columns of the Intake Form.
2. The state saves related evidence and artifacts in a securely shared repository, accessible to CMS reviewers.
3. At least two weeks before the ORR, the state sends the completed Intake Form to the CMS State Officer and to MES@cms.hhs.gov, giving CMS access to the evidence in the repository.
4. Prior to the ORR, CMS will review the evidence, compile a list of any preliminary questions, and send those to the state to address during the ORR session.

The ORR review session is divided into two segments: 1) a state presentation and 2) a question and answer (Q&A) session. During the first segment, the state will provide a succinct project overview and demonstration (via testing results, live demonstrations, other evidence, etc.). The state should indicate how the system collects the data necessary for metrics reporting (described in the APD/APD-U) to validate the continued health of the system post-production. For states with an approved APD/APD-U that does not define specific metrics, states should collaborate with CMS to define project metrics as part of ORR preparation. The Q&A session provides CMS reviewers time to ask additional questions based on information provided before and during the ORR session. Because the ORR focuses on both outcome achievement and system deployment, CMS encourages states to include appropriate subject matter experts from program, business operations, and IT.

After the ORR, CMS will enter comments into the Intake Form and return it to the state. The state should continue working with their CMS State Officer on addressing ORR observations and findings as the project goes into production, and in preparation for the CR.

PRODUCTION PHASE: REQUESTING A CERTIFICATION REVIEW

To request a CR, states must submit an Official Certification Request Letter that includes:

- The date at which the system became the system of record
- The date back to which the state is requesting the system be certified
- A proposed timeframe for the review

The letter must be accompanied by information that demonstrates the state is ready to be certified. Readiness means that the state has:

- Submitted all metrics related to the project being certified, up to the most recent quarter
- Established a document repository that has been successfully tested by the CMS State Officer (the default repository is CMS Box)
- Submitted a copy of the System Acceptance Letter (the state's letter to the vendor contractor or state development team accepting the system/modules(s))
- Submitted an operational report, if needed
- Demonstrated that the MES module requesting certification meets all applicable security controls and requirements
- Demonstrated that the MES module requesting certification complies with T-MSIS requirements:

- The state maintains monthly production submissions of T-MSIS files (states will be deemed out of compliance with timeliness requirements if T-MSIS files are submitted later than one month after the T-MSIS reporting period).
- The state maintains complete and accurate historical T-MSIS data for program evaluation and the continuous improvement in business operations pursuant to 42 C.F.R. §433.112(b)(15).
- The state can demonstrate that data quality issues are meeting the targets for Outcomes Based Assessment (OBA) critical priority data quality checks, high priority data quality checks, and the expenditure data content category. The state should also demonstrate they are working in good faith to resolve such issues. Generally, CMS will consider the state out of compliance with T-MSIS requirements if it is not meeting the targets for OBA criteria in critical priority data quality checks, high priority data quality checks, and the expenditure data content category and/or the state is not working in good faith to resolve any identified data quality issues.
- The state meets all requirements outlined in the T-MSIS Reporting - Standard Operating Procedures (SOP) for any Large System Enhancements (LSEs) affecting T-MSIS reporting.

The CR will also focus on metrics. Metrics, along with any underlying data and explanatory or contextual information, should be sent to the CMS State Officer and to MES@cms.hhs.gov. The state and CMS State Officer will agree upon the format for reporting. In the future, CMS may issue a template for reporting on metrics. CMS may send questions about the metrics to the state prior to the CR.

PRODUCTION PHASE: CERTIFICATION REVIEW

Once the system has been in production for at least 6 months, and the state can report on approved metrics, a CR will be conducted with their CMS State Officer. A CR is necessary for the state to receive enhanced federal funding for system maintenance and operations. The state should schedule the CR with their CMS State Officer well in advance to prepare for the CR and collaboratively define the scope of the review. We reiterate the importance of frequent conversations between the state and their CMS State Officer. The state will need to demonstrate – with appropriate evidence – that the approved CMS-required and state-specific outcomes and metrics are being achieved by the system in production. In contrast to the ORR (which is focused on the demonstration of functionality associated with the applicable CMS-required and state-specific outcomes in pre-production), the CR is focused on demonstrating the impact of functionality in production, as assessed by metrics.

As with the ORR, any required legal non-disclosure and data-sharing agreements should be prepared for the review of the relevant module.

During the CR, states will demonstrate to CMS that the system in production achieves the value described in the APD/APD-U. As with the ORR, CMS encourages states to include all appropriate program, business operations, and IT subject matter experts are present for the CR.

For the CR, the following steps are completed:

1. The state completes the state columns of the Intake Form.
2. The state saves related evidence and artifacts in a securely shared repository, accessible to CMS reviewers.
3. At least two weeks before the CR, the state sends the completed Intake Form to the CMS State Officer and to MES@cms.hhs.gov, giving CMS access to the evidence in the repository.

4. Prior to the CR, CMS will review the evidence, compile a list of questions, and send them to the state to be addressed during the CR session.

The CMS State Officer will communicate what, if any, evidence supporting the Conditions for Enhanced Funding or outcomes that the state should upload to the state repository prior to the CR, and work with the state to agree upon demonstrations of system functionality that will be provided during the CR. In addition, states will clearly describe and display to CMS the metrics used to validate the continued health of the system post-production.

The CR will include a review of CMS findings from the ORR and identify any operational issues experienced since entering production. Discussions will focus on how these issues have been handled or resolved, highlighting any associated workarounds, as well as demonstrating the state's measured progress to resolve them (including live demonstrations of functionality, as needed).

As with the ORR, the CR is divided into two segments: 1) the state presentation and 2) a question and answer (Q&A) session. During the first segment, the state will concisely demonstrate or otherwise provide evidence of functionality related to the outcomes and their aligned programmatic value. The state will discuss ORR findings and operational issues that surfaced since the ORR, as well as discuss how the respective metrics demonstrate that the project is achieving outcomes. During the Q&A segment, the state responds to CMS questions and discusses how successfully the system is supporting the state's operational needs and goals.

CMS will follow-up with the state shortly after the CR to discuss any findings, as applicable. Additionally, CMS will comment about the review in the final CR report returned to the state along with a formal CR Decision Letter.

OPERATIONAL REPORTING PHASE (ONGOING)

To efficiently demonstrate ongoing, successful system operations, states must submit operational reports containing data and/or other evidence that modules are meeting all applicable requirements for the state's claimed federal matching funds. These reports should be submitted annually in support of the OAPD request; however, more frequent reporting on key operational metrics may be necessary. Operational reports should include metric data corresponding to the agreed-upon intended outcomes for each applicable MES module. In addition to operational reports, states must submit an OAPD per 45 C.F.R. §95.611, for enhanced funding authorized through certification at 42 C.F.R. §433.116 for any module or system for which the state requests enhanced federal matching funds for the state's expenditures on operations of an existing system.

States should coordinate with their CMS State Officers to determine which modules and metrics may need more frequent reporting. The operational reports should include the same level of streamlined information described above:

- Compliance with the Conditions for Enhanced Funding required under 42 C.F.R. §433.112 and §433.116
- Outcomes
- Metrics (and related supporting evidence)

States should look to standardize frequency of reported metrics over time. States should submit all data in table form, with numerators and denominators present, in an Excel document that can be tracked

longitudinally with new columns added each reporting period and which explains contextual information on what was achieved in the metric.

For previously certified systems, those operating as a system of record, and/or those for which the state is claiming enhanced federal matching funds for DDI or operations, states should coordinate with their respective CMS State Officers to agree upon an approach and schedule to begin operational reporting.

Regulations at 42 C.F.R. §433.119 indicate that CMS may periodically review and reapprove each system initially approved under 42 C.F.R.§433.114 for 75 percent enhanced federal matching for state expenditures on the system's ongoing operations. CMS may review an entire system's or module's operation or focus the review on the operation of limited parts of the system or module. However, at a minimum, CMS reviews under 42 C.F.R. §433.119 will look to validate that the system is operating in alignment with all applicable regulatory requirements and may give particular attention to regulatory reapproval conditions on which the system or module demonstrated weakness in previous reviews. In general, the reapproval process will be consistent with the Streamlined Modular Certification process outlined in this SMDL.

TRANSITION TO STREAMLINED MODULAR CERTIFICATION

REPLACING THE MECT AND MEET

The MECT was implemented in 2007 through CMS guidance and contains business areas relevant to the Medicaid Management Information System (MMIS) functions to process claims for services furnished to beneficiaries and to perform other functions necessary for the Medicaid program's economic and efficient operations, management, monitoring, and administration. CMS guidance on MECT was also designed to assist states as they plan, develop, test, and implement their MMIS. CMS updated the MECT guidance in 2016.[2] Later, in 2017, CMS issued the MEET to assist states in streamlining and modernizing their Eligibility and Enrollment (E&E) systems.[3]

Since the release of the MECT and MEET, feedback from states at system reviews and certifications, and through other channels, has indicated that the MECT and MEET have been overly burdensome for states, lack the flexibility states need to best implement systems to support program priorities, and are not adequately focused on how the projects will improve a state's Medicaid program.

As a result of this state feedback, as well as lessons learned from the OBC experience (which significantly reduced burden for states and CMS), similar lessons learned from state pilots, and CMS's own experience, CMS will no longer be relying on the MECT and MEET frameworks for system certification.[4]

With the release of the updated Certification Guidance accompanying this SMDL replacing the MECT and MEET toolkits, CMS and states will begin transitioning to the Streamlined Modular Certification process for current and future MES projects. States should work with their CMS State Officers to

[2] https://www.medicaid.gov/medicaid/data-systems/medicaid-eligibility-enrollment-toolkit/index.html

[3] https://www.medicaid.gov/medicaid/data-systems/medicaid-eligibility-enrollment-toolkit/index.html

[4] Based on evidence gathered during a pilot test of the initial OBC process, the pilot state saw an 87 percent burden reduction in terms of staff time for certification. CMS anticipates that the SMC process will see similar levels of burden reduction.

determine the best path forward and smoothest transition process. States that are significantly far along in their preparations for module certification under the MECT or MEET framework may elect to proceed with certification under the relevant legacy certification toolkit. However, states that elect to do so will also be expected to produce and submit operational reports for their systems.

This updated Certification Guidance contains several key elements which were not present in MECT and MEET. These elements include outcomes, metrics, and operational reporting requirements (including indicators of project health). In addition, milestone reviews under Streamlined Modular Certification differ substantially from those required under the toolkits. As such, states should consider these key elements and differences in transition planning efforts. States should work with their CMS State Officers to coordinate the transition to Streamlined Modular Certification.

MITA STATE SELF-ASSESSMENTS

Under current regulations at 42 C.F.R. §433.112(b)(11) and §433.116(b), (c), and (i), and guidance issued by CMS in 2014,[5] states are required to submit a MITA State Self-Assessment (SS-A) in support of their request for enhanced federal matching for their MES expenditures. As part of CMS's focus on outcomes and reducing administrative burden, CMS will accept an alternative format for the MITA State Self-Assessment (SS-A), if preferred. In place of focusing on rating the maturity level of a state's MES across each MITA business area, the SS-A could include the following information:

- Current operational problems and risks, challenges, and limitations of the existing system or module,
- Which Medicaid program goals are impacted by the existing system or module limitations and the nature of the impact; and
- Definition of what success looks like in the To-Be state and how it will be measured.

CONCLUSION

This Certification Guidance is a critical component in streamlining and moving towards an OBC process for enhanced funding of state MES projects. This Certification Guidance reflects reduced burden and increased flexibility for states while ensuring states are meeting all federal requirements (and state-specific outcomes) for these systems. This guidance also emphasizes a model of frequent collaboration between CMS and states. Adherence to these improved processes will not only help ensure that state and federal investments are worthwhile, but that Medicaid beneficiaries and other stakeholders benefit from the efficient, economical, and effective administration of the state's Medicaid program through these systems.

[5] *CMCS Informational Bulletin*, "Medicaid Information Technology Architecture (MITA) Guidance – Eligibility and Enrollment Supplement, Version 3.0," August 5, 2014. https://www.medicaid.gov/federal-policy-guidance/downloads/CIB-08-05-2014.pdf.

APPENDIX A: CONDITIONS FOR ENHANCED FUNDING

The information in the following table contains the Conditions for Enhanced Funding (CEF) described in 42 C.F.R. §433.112 that are applicable for all MES modules.

This table, combined with the applicable table(s) in ***Appendix B: CMS-Required Outcomes for Specific MES Modules***, are a starting point for aligning the state's goals for a project with applicable CMS-required outcomes.

Table A-1: Conditions for Enhanced Funding (CEF)

Ref #	Condition
1	CMS determines the system is likely to provide more efficient, economical, and effective administration of the State plan.
2	The system meets the system requirements, standards and conditions, and performance standards in Part 11 of the State Medicaid Manual, as periodically amended.
3	The system is compatible with the claims processing and information retrieval systems used in the administration of Medicare for prompt eligibility verification and for processing claims for persons eligible for both programs.
4	The system supports the data requirements of quality improvement organizations established under Part B of title XI of the Act.
5	The State owns any software that is designed, developed, installed or improved with 90 percent FFP.
6	The Department has a royalty-free, non-exclusive, and irrevocable license to reproduce, publish, or otherwise use and authorize others to use, for Federal Government purposes, software, modifications to software, and documentation that is designed, developed, installed or enhanced with 90 percent FFP.
7	The costs of the system are determined in accordance with 45 C.F.R 75, subpart E.
8	The Medicaid agency agrees in writing to use the system for the period of time specified in the advance planning document (approved by CMS) or for any shorter period of time that CMS determines justifies the Federal funds invested.
9	The agency agrees in writing that the information in the system will be safeguarded in accordance with subpart F, part 431 of this subchapter.
10	Use a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces; the separation of business rules from core programming, available in both human and machine readable formats.
11	Align to, and advance increasingly, in maturity for business, architecture, and data.
12	The agency ensures alignment with, and incorporation of, industry standards adopted by the Office of the National Coordinator for Health IT in accordance with 45 C.F.R. part 170, subpart B: The HIPAA privacy, security and transaction standards; accessibility standards established under section 508 of the Rehabilitation Act, or standards that provide greater accessibility for individuals with disabilities, and compliance with Federal civil rights laws; standards adopted by the Secretary under section 1104 of the Affordable Care Act; and standards and protocols adopted by the Secretary under section 1561 of the Affordable Care Act.

Ref #	Condition
13	Promote sharing, leverage, and reuse of Medicaid technologies and systems within and among States.
14	Support accurate and timely processing and adjudications/eligibility determinations and effective communications with providers, beneficiaries, and the public.
15	Produce transaction data, reports, and performance information that would contribute to program evaluation, continuous improvement in business operations, and transparency and accountability.
16	The system supports seamless coordination and integration with the Marketplace, the Federal Data Services Hub, and allows interoperability with health information exchanges, public health agencies, human services programs, and community organizations providing outreach and enrollment assistance services as applicable.
17	For E&E systems, the State must have delivered acceptable MAGI-based system functionality, demonstrated by performance testing and results based on critical success factors, with limited mitigations and workarounds.
18	The State must submit plans that contain strategies for reducing the operational consequences of failure to meet applicable requirements for all major milestones and functionality. This should include, but not be limited to, the Disaster Recovery Plan and related Disaster Recovery Test results.
19	The agency, in writing through the APD, must identify key state personnel by name, type and time commitment assigned to each project.
20	Systems and modules developed, installed or improved with 90 percent match must include documentation of components and procedures such that the systems could be operated by a variety of contractors or other users.
21	For software systems and modules developed, installed or improved with 90 percent match, the State must consider strategies to minimize the costs and difficulty of operating the software on alternate hardware or operating systems.
22	Other conditions for compliance with existing statutory and regulatory requirements, issued through formal guidance procedures, determined by the Secretary to be necessary to update and ensure proper implementation of those existing requirements.

APPENDIX B: CMS-REQUIRED OUTCOMES FOR SPECIFIC MES MODULES

The following tables contain the CMS-required outcomes for specific MES modules. These outcomes are aligned with statutory, regulatory and policy requirements that states must follow when implementing modules or capabilities. These are a starting point for aligning the state's project goals with applicable CMS outcomes. The list should be adjusted if any outcomes are deemed not applicable for a state project or if the state proposes other outcomes that are not covered in the applicable table(s) below.

Table B-1: Eligibility and Enrollment (E&E) Outcomes

Reference #	Outcome	Source(s)
EE1	The eligibility system receives, ingests, and processes the single-streamlined applications, change of circumstances, renewal forms, and any supporting documentation requested by the state (including telephonic signatures) from individuals, for all Medicaid eligibility groups and CHIP through online via multiple browsers, mail (paper), phone, and in-person (e.g., via kiosk) applications to support eligibility determination for all Insurance Affordability Programs (Federal Health Insurance Exchange), state Medicaid or CHIP, State-Based Marketplace (SBM), Basic Health Program (BHP).	42 C.F.R. §435.907 42 C.F.R. §435.916 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE2	Individuals experience a user-friendly, dynamic, online application, such that subsequent questions are based on prior answers.	42 C.F.R. §435.907 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE3	Individuals eligible for automatic Medicaid eligibility are promptly enrolled (e.g., SSI recipients in 1634 states, individuals receiving a mandatory state supplement under a federally- or state-administered program, individuals receiving an optional State supplement per 42 C.F.R. 435.230 and deemed newborns). (Automatic enrollment in Guam, Puerto Rico, and the U.S. Virgin Islands is required only for individuals receiving cash assistance under a state plan for OAA, AFDC, AB, APTD, or AABD, and deemed newborns.)	42 C.F.R. §435.117 42 C.F.R. §435.909 42 C.F.R. §436.909 and 42 C.F.R. §436.124 (for Guam, Puerto Rico, and the Virgin Islands)
EE4	The state correctly calculates income and household composition based on Modified Adjusted Gross Income (MAGI) and non-MAGI methodologies at application and renewal. Example business rules include subtracting 5 percentage points off FPL for applicable family size.	42 C.F.R. §435.603 42 C.F.R. §436.601 and 42 C.F.R. §436.811-814 (for Guam, Puerto Rico, and the Virgin Islands)

Reference #	Outcome	Source(s)
EE5	The eligibility system uses automated interfaces with electronic data sources to enable real-time or near real-time, no manual touch eligibility determinations. The data sources include (but are not limited to) SSA and the Department of Homeland Security (DHS) (directly or via the Federal Data Services Hub (FDSH)), state quarterly wage data, data from financial institutions for asset verification, Renewal and Redetermination Verification service through the FDSH, Public Assistance Reporting Information System (PARIS) to verify Medicaid coverage in other states.	42 C.F.R. §435.940-965 42 C.F.R. §435.945(d) 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE6	Individuals who apply for Medicaid based on disability receive an eligibility determination within 90 days and all other applicants receive an eligibility determination within 45 days.	42 C.F.R. §435.911-912 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE7	Individuals are enrolled for up to 90 days if pending verification of citizenship or immigration status.	42 C.F.R. §435.407 42 C.F.R. §435.956 42 C.F.R. §436.407 and §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE8	Individuals are enrolled pending verification of SSN.	42 C.F.R. §435.910 42 C.F.R. §435.956(d) 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE9	Individuals receive system-generated timely automated (versus manual) eligibility notices and request for additional information for eligibility determination, as necessary.	42 C.F.R. §431.210-214 42 C.F.R. §435.917-918 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE10	Individuals receive electronic notices and alerts as applicable via their preferred mode of communication (e.g., email, text that notice is available in online account).	42 C.F.R. §431.210-214 42 C.F.R. §435.917-918 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE11	Following an eligibility determination, the system promptly sends the beneficiary information to MMIS to complete enrollment into the appropriate delivery system (e.g., FFS, managed care).	42 C.F.R. §435.914 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE12	The system receives Presumptive Eligibility (PE) applications from all approved entities in an automated manner and facilitates eligibility termination if no full Medicaid application is received by the end of the month following the month of PE determination.	42 C.F.R. §435.1110

Reference #	Outcome	Source(s)
EE13	The system uses electronic data sources to confirm eligibility, wherever possible, to facilitate ex-parte renewals.	42 C.F.R. §435.916 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE14	If ex-parte renewal cannot be completed, the system can automatically generate pre-populated renewal forms and distribute those forms via individuals' preferred communication mode.	42 C.F.R. §435.916 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE15	The system applies an automated eligibility hierarchy that places an individual in the most advantageous group for which they are eligible at initial application and renewal.	42 C.F.R. §435.404 42 C.F.R. §436.404 (for Guam, Puerto Rico, and the Virgin Islands)
EE16	The system uses automated business rules to assign accurate eligibility categories for all the mandatory and relevant optional eligibility groups at initial application and renewal. Example business rules include: • Correct identification of individuals age 19-64 at or below 133 percent FPL (VIII group) • Correct alignment of eligibility categories to FMAP rate	42 C.F.R. §435.404 42 C.F.R. §436.404 (for Guam, Puerto Rico, and the Virgin Islands)
EE17	Incarcerated individuals receive timely access to inpatient services and receive a timely and accurate eligibility determination upon release.	42 C.F.R. §435.1009 42 C.F.R. §436.1005 (for Guam, Puerto Rico, and the Virgin Islands)
EE18	Individuals whose coverage is limited to emergency services due to immigration status receive timely and accurate eligibility determination.	42 C.F.R. §435.139 42 C.F.R. §440.255(c) 42 C.F.R. §436.128 (for Guam, Puerto Rico, and the Virgin Islands)
EE19	Individuals receive timely and accurate determinations of eligibility for the three months prior to the date of application if the individual would have been eligible and received Medicaid covered services.	42 C.F.R. §435.915 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE20	Individuals are promptly enrolled with the accurate effective date of eligibility in accordance with the approved State Plan.	42 C.F.R. §435.915 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE21	In states that have an integrated eligibility system with human services programs, the system is able to pend application for one program without having to do so for Medicaid or CHIP programs, if needed.	June 18, 2013, CMS Guidance on State Alternative Applications for Health Coverage
EE22	The state maintains a coordinated eligibility and enrollment process with all insurance affordability programs by supporting bi-directional data-sharing for application-related data and adjudication status with all relevant insurance affordability programs (FFE, CHIP, SBE if applicable, BHP if applicable).	42 C.F.R. §435.1200

Reference #	Outcome	Source(s)
EE23	Account Transfer information for individuals applying at the FFE from a determination state is automatically ingested and the state promptly enrolls individuals determined eligible by the FFE.	42 C.F.R. §435.1200
EE24	Account Transfer information for individuals applying at the FFE from an assessment state is automatically ingested and the state conducts only the remaining verifications necessary to complete the determination process for individuals assessed as potential eligible by the FFE.	42 C.F.R. §435.1200
EE25	The system receives and responds to requests from the FFE in real-time to confirm whether an individual applying for coverage through the FFE currently has Minimum Essential Coverage through Medicaid or CHIP.	42 C.F.R. §435.1200
EE26	Persons with disabilities or with Limited English Proficiency (LEP) can submit a single, streamlined application with any necessary assistance (e.g., TTY for the hearing impaired for phone applications, and language assistance for persons with LEP).	42 C.F.R. §435.905 42 C.F.R. §435.908 42 C.F.R. §436.901 (for Guam, Puerto Rico, and the Virgin Islands)
EE27	Beneficiaries and applicants can submit an appeal against an adverse action via multiple channels (e.g., online, phone, mail, in person) and the appeal status and adjudication of an appeal can easily be accessed by necessary state staff and appellants.	42 C.F.R. §431.221

Table B-2: Claims Processing Outcomes

Reference #	Outcome	Source(s)
CP1	The system receives, ingests, and retains claims, claims adjustments, and supporting documentation submitted both electronically and by paper in standard formats.	45 C.F.R. §162.1102
CP2	The system performs comprehensive validation of claims and claims adjustments, including validity of services.	42 C.F.R. §431.052 42 C.F.R. §431.055 42 C.F.R. §447.26 42 C.F.R. §447.45(f) 45 C.F.R. §162.1002 SMD Letter 10-017 SMM Part 11 Section 11300

Reference #	Outcome	Source(s)
CP3	The system confirms authorization for services that require prior approval to manage costs or ensure patient safety, and that the services provided are consistent with the authorization. The system accepts use of the authorization by multiple sequential providers during the period as allowed by state rules. Prior-authorization records stored by the system are correctly associated with the relevant claim(s).	SSA 1927(d)(5) 42 C.F.R. §431.630 42 C.F.R. §431.960 45 C.F.R. §162.1302 SMM Part 4 SMM Part 11 Section 11325
CP4	The system correctly calculates payable amounts in accordance with the State Plan and logs accounts payable amounts for payment processing. The system accepts, adjusts, or denies claim line items and amounts and captures the applicable reason codes.	42 C.F.R. §431.052
CP5	The state communicates claims status throughout the submission and payment processes and in response to inquiry. If there are correctable errors in a claims submission, the system suspends the claims, attaches pre-defined reason code(s) to suspended claims, and communicates those errors to the provider for correction. The system associates applicable error or reason code(s) for all statuses (e.g., rejected, suspended, denied, approved for payment, paid) and communicates those to the submitter. The system shows providers, case managers and members current submission status through one or more of the following: • Automatic notices, as appropriate, based on claims decision or suspension. • Explanation of Benefits (EOB). • Providing prompt response to inquiries regarding the status of any claim through a variety of appropriate technologies and tracking and monitoring responses to the inquiries. • Application programming interface (API)	45 C.F.R. §162.1402 (c) 45 C.F.R. §162.1403 (a) & (b) 42 C.F.R. §431.60 (a) & (b) SMM Part 11 Section 11325
CP6	The system tracks each claim throughout the adjudication process (including logging edits made to the claim) and retains transaction history to support claims processing, reporting, appeals, audits, and other uses.	42 C.F.R. §447.45 42 C.F.R. §431.17 SMM Part 11 Section 11325

Table B-3: Financial Management Outcomes

Reference #	Outcome	Source(s)
FM1	The system calculates FFS provider payment or recoupment amounts, as well as value-based and alternative payment models (APM), correctly and initiates payment or recoupment action as appropriate.	Section 1902(a)(37) of the Act 42 C.F.R. §433.139 42 C.F.R. §447.20 42 C.F.R. §447.45 42 C.F.R. §447.56 42 C.F.R. §447.272
FM2	The system pays providers promptly via direct transfer and electronic remittance advice or by paper check and remittance advice if electronic means are not available.	42 C.F.R. §447.45 42 C.F.R. §447.46
FM3	The system supports the provider appeals by providing a financial history of the claim along with any adjustments to the provider's account resulting from an appeal.	42 C.F.R. §431.152
FM4	The system accurately pays per member/per month capitation payments electronically in a timely fashion. Payments account for reconciliation of withholds, incentives, payment errors, beneficiary cost sharing, and any other term laid out in an MCO contract.	42 C.F.R. §438 42 C.F.R. §447.56(d)
FM5	The system accurately tallies recoupments by tracking repayments and amounts outstanding for individual transactions and in aggregate for a provider.	42 C.F.R. §447
FM6	The state recovers third party liability (TPL) payments by: • Tracking individual TPL transactions, repayments, outstanding amounts due, • Aggregating by member, member type, provider, third party, and time period, • Alerting state recovery units when appropriate, and • Electronically transferring payments to the state.	42 C.F.R. §433.139
FM7	The system processes drug rebates accurately and quickly.	42 C.F.R. §447.509
FM8	State and federal entities receive timely and accurate financial reports (cost reporting, financial monitoring, and regulatory reporting), and record of all transactions according to state and federal accounting, transaction retention, and audit standards.	42 C.F.R. §431.428 42 C.F.R. §433.32

Reference #	Outcome	Source(s)
FM9	The system tracks that Medicaid premiums and cost sharing incurred by all individuals in the Medicaid household does not exceed an aggregate limit of five percent of the family's income. If the beneficiaries at risk of reaching the aggregate family limit, the system tracks each family's incurred premiums and cost sharing without relying on beneficiary documentation.	42 C.F.R. §447.56(f)

Table B-4: Decision Support System (DSS)/Data Warehouse (DW) Outcomes

Reference #	Outcome	Source(s)
DSS/DW1	The system supports various business processes' reporting requirements	42 C.F.R. §431.428
DSS/DW2	The solution includes analytical and reporting capabilities to support key policy decision making	42 C.F.R. §433.112

Table B-5: Encounter Processing System (EPS) Outcomes

Reference #	Outcome	Source(s)
EPS1	The system ingests encounter data (submissions and re-submissions) from MCOs and sends quality transaction feedback back to the plans to ensure appropriate industry standard format. (Quality transaction checks include, but are not limited to completeness, missing information, formatting, and the TR3 implementation guide business rules validations).	42 C.F.R. §438.242
EPS2	The system ingests encounter data (submissions and re-submissions) from managed care entities in compliance with HIPAA security and privacy standards and performing quality checks for completeness and accuracy before submitting to CMS using standardized formatting, such as ASC X12N 837, NCPDP and the ASC X12N 835, as appropriate. (Quality checks include, but are not limited to completeness, character types, missing information, formatting, duplicates, and business rules validations, such as payment to dis-enrolled providers, etc.).	42 C.F.R. §438.604 42 C.F.R. §438.818 42 C.F.R. §438.242
EPS3	The state includes submission requirements (timeliness, re-submissions, etc.), definitions, data specifications and standards, and consequences for non-compliance in its managed care contracts. The state enforces consequences for non-compliance.	42 C.F.R. §438.3
EPS4	The state uses encounter data to calculate capitation rates and performs payment comparisons with FFS claims data.	42 C.F.R. §438
EPS5	The state complies with federal reporting requirements.	42 C.F.R. §438.818 42 C.F.R. §438.242

Table B-6: Long Term Services & Supports (LTSS) Outcomes

Reference #	Outcome	Source(s)
LTSS1	LTSS system generates notifications including eligibility determination; termination of state waiver (30 days in advance); and inspections taking place in a beneficiary's home when a beneficiary receives services in his/her own home or the home of a relative (HCBS waiver for individuals 65 and older) (48 hours in advance).	42 C.F.R. §441.307 42 C.F.R. §441.356 42 C.F.R. §441.365 42 C.F.R. §431.206 42 C.F.R. §431.210 42 C.F.R. §433.112
LTSS2	LTSS systems stores proof of beneficiary consent to enroll in HCBS state plan or waiver-based programs.	42 C.F.R. §441.301
LTSS3	LTSS system assigns, tracks and changes beneficiary prioritization and waiver waitlist status.	42 C.F.R. §433.112
LTSS4	LTSS system maintains a record of beneficiaries who have left the waiver program due to death or loss of eligibility for Medicaid under the State Plan to replace those beneficiaries with others on the waitlist.	42 C.F.R. §441.305
LTSS5	LTSS system stores the person-centered plan, including any updates or changes containing all required information and consent signatures.	42 C.F.R. §441.302
LTSS6	LTSS system supports conflict-free case management via role-based access, proper firewalls, and mitigation strategies that provide beneficiaries appropriate access to records.	HIPAA 42 C.F.R. §441.301
LTSS7	LTSS System supports completion of CMS Form 372.	42 C.F.R. §433.112 42 C.F.R. §441.302
LTSS8	LTSS system collects and saves prior authorizations to exchange with MMIS as needed to prevent the provision of unnecessary or inappropriate services and supports.	42 C.F.R. §441.301
LTSS9	LTSS system documents and tracks reportable events related but not limited to instances of abuse, neglect, exploitation, and unexplained death from case initiation to case closeout.	42 C.F.R. §441.404 42 C.F.R. §441.585 42 C.F.R. Part 438 CMS Bulletin, Modifications to Quality Measures and Reporting in §1915(c) Home and Community-Based Waivers, March 12, 2014
LTSS10	LTSS system collects grievances related but not limited to instances of abuse, neglect, exploitation, and unexplained death from case initiation to case closeout.	42 C.F.R. §441.464 42 C.F.R. §441.555

Reference #	Outcome	Source(s)
LTSS11	LTSS system creates trend reports of critical incident causes and tracks trends of critical incidents after operational implementation of interventions/mitigations/corrective actions.	Application for a §1915(c) Home and Community-Based Waiver [Version 3.6, January 2019] Instructions, Technical Guide and Review Criteria p.242-243 (Appendix G-1-e) Modifications to Quality Measures and Reporting in §1915(c) Home and Community-Based Waivers, Page 10

Table B-7: Member Management Outcomes

Reference #	Outcome	Source(s)
MM1	The system auto-assigns managed care enrollees to appropriate managed care organizations, per state and federal regulations.	42 C.F.R. §438.54
MM2	The system sends notice, or facilitates, to the enrolled member with an initial assignment, a reasonable period to change the selection, and appropriate information needed to make an informed choice. If no selection is made, the system either confirms the original assignment, or assigns the member to FFS.	42 C.F.R. §438.10 42 C.F.R. §438.54
MM3	The system disenrolls members at the request of the plan and in accordance with state procedures.	42 C.F.R. §438.56(b), (c), and (d)
MM4	Disenrollments are effective in the system the first day of the second month following the request for disenrollment.	42 C.F.R. §438.56(e)
MM5	The system notifies enrollees of their disenrollment rights at least 60 days before the start of each enrollment period. This notification is in writing.	42 C.F.R. §438.56(f)
MM6	To prevent duplication of activities, enrollee's needs are captured by the system so that MCOs, PIHPs, and PAHPs can see and share the information (in accordance with privacy controls).	42 C.F.R. §438.208(b)
MM7	The system allows beneficiaries or their representative to receive information through multiple channels including phone, Internet, in-person, and via auxiliary aids and services.	42 C.F.R. §438.71

Reference #	Outcome	Source(s)
MM8	The state provides content required by 42 C.F.R. 438.10, including but not limited to definitions for managed care and enrollee handbook, through a website maintained by the state.	42 C.F.R. §438.10(c)
MM9	Potential enrollees are provided information about the state's managed care program when the individual become eligible or is required to enroll in a managed care program. The information includes, but is not limited to the right to disenroll, basic features of managed care, service area coverage, covered benefits, and provider directory and formulary information.	42 C.F.R. §438.10(e)
MM10	The system maintains an up-to-date (updated at least annually) fee-for-service (FFS) or primary care case-management (PCCM) provider directory containing the following: • Physician/provider • Specialty • Address and telephone number • Whether the physician/provider is accepting new Medicaid patients (for PCCM providers), and • The physician/provider's cultural capabilities and a list of languages supported (for PCCM providers).	Section 1902(a)(83) 1902(mm) SMD # 18-007
MM11	The system captures enough information such that the state can evaluate whether members have access to adequate networks. (Adequacy is based on the state's plan and federal regulations).	42 C.F.R. §438.68

Table B-8: Prescription Drug Monitoring Program (PDMP) Outcomes

Reference #	Outcome	Source(s)
PDMP1	Covered providers have near real-time access to: a. Information regarding Medicaid beneficiary's prescription drug history. b. The number and type of controlled substances prescribed to and filled for the covered individual during at least the most recent 12-month period. c. The name, location, and contact information (or other identifying number selected by the state, such as a national provider identifier issued by the CMS National Plan and Provider Enumeration System) of each covered provider who prescribed a controlled substance to the covered individual during at least the most recent 12-month period.	Section 1944(b) of the Act Section 5042 – Medicaid PARTNERSHIP Act CMS FAQs-SUPPORT for Patients and Communities Act

Reference #	Outcome	Source(s)
PDMP2	Providers can easily use the PDMP information though workflow integration, which may include electronic prescribing system for controlled substances.	Section 1944(b) of the Act Section 5042 – Medicaid PARTNERSHIP Act CMS FAQs-SUPPORT for Patients and Communities Act
PDMP3	The state has data-sharing agreements with all contiguous states to track patients, prescribers, and prescriptions across state lines.	Section 1944(f) of the Act Section 5042 – Medicaid PARTNERSHIP Act CMS FAQs-SUPPORT for Patients and Communities Act
PDMP4	The state medical and pharmacy directors and any designee has access to the PDMP information in an electronic format based on data-sharing agreements in place (subject to state law).	Section 1944(b) of the Act Section 5042 – Medicaid PARTNERSHIP Act CMS FAQs-SUPPORT for Patients and Communities Act
PDMP5	The state produces data for the reports that are required to be submitted in the Annual Report to HHS.	Section 1944(e) of the Act Section 5042 – Medicaid PARTNERSHIP Act 42 C.F.R. §433.112(b)(15) CMS FAQs-SUPPORT for Patients and Communities Act
PDMP6	The system produces reports to contribute to reports to HHS by the State Drug Utilization Review (DUR) Board and for program evaluation, continuous improvement in business operations, transparency and accountability, as well as identify patterns of fraud, abuse, gross overuse, excessive utilization related to limitations identified by the state, inappropriate or medically unnecessary care, or prescribing or billing practices that indicate abuse or excessive utilization among Medicaid physicians, pharmacists and enrollees associated with specific drugs or groups of drugs.	Section 1944 (e)(1) of the Act Section 1927(g)(2)(B) and (g)(3)(D) of the Act Section 1004 of the SUPPORT Act 42 C.F.R. §433.112(b)(15) CMS FAQs-SUPPORT for Patients and Communities Act Centers for Disease Control

Table B-9: Pharmacy Benefit Management (PBM) Outcomes

Reference #	Outcome	Source(s)
PBM1	The system adjudicates claims within established time parameters to ensure timely pharmacy claims payments.	Section 1927(h) of the SSA 42 C.F.R. §456.722

Reference #	Outcome	Source(s)
PBM2	The system adjudicates claims accurately within established parameters. The module can be configured to provide authority/ability to override a reject/edit/denied claim and then resubmit to ensure timely provider claims payments.	42 C.F.R. §456.722
PBM3	The system captures the necessary data to ensure timely processing of manufacturer rebates as well as the capability to track rebates to promote beneficiary cost savings.	Section 1927 of the SSA 42 C.F.R. §447.509
PBM4	The system has the capability to support cost savings by capturing, storing, and transferring data to the payment process system to generate invoices of participating drug manufacturers within 60 days of the end of each quarter.	Section 1927(b)(2) of the SSA 42 C.F.R. §447.520 42 C.F.R. §447.511
PBM5	The system supports cost savings by enabling the tracking, monitoring, and reporting of manufacturer's pharmacy drugs and rebate savings.	Section 1927(b)(2) of the SSA 42 C.F.R. §447.520 42 C.F.R. §447.511
PBM6	The system enables the beneficiary to have timely access to medication if the system has the capability to perform prior authorization and provide a response by telephone or other telecommunication devices within 24 hours of a request and provides for the dispensing of at least 72-hour supply of a covered outpatient prescription drug in an emergency situation (unless excluded under the SSA).	Section 1927(d)(5) of the SSA
PBM7	The system supports CMS oversight of the safe, effective, and appropriate dispensing of medications by enabling the capability to provide data to support the creation of the CMS annual report on the operation and status of the state's DUR program.	Section 1927(g)(3)(D) of the SSA Section 1944(e)(1) of the SSA 42 C.F.R. §456.712
PBM8	The system supports the safe, effective, and appropriate dispensing of medications by enabling the capability to provide point-of-sale or point of distribution prospective review of drug therapy based upon predetermined standards, including standards for counseling.	Section 1927 (g) of the SSA 42 C.F.R. §456.703 42 C.F.R. §456.705(b) 42 C.F.R. §456.709
PBM9	The system supports the identification of patterns of fraud, abuse, gross overuse, or inappropriate or medically unnecessary care, or prescribing or billing practices indicating abuse or excessive utilization among physicians, pharmacists and individuals receiving benefits by enabling the collection of pharmacy data to be used in retrospective drug utilization reviews.	Section 1927 (g) of the SSA 42 C.F.R. §456.703 42 C.F.R. §456.705(b) 42 C.F.R. §456.709

Table B-10: Provider Management Outcomes

Reference #	Outcome	Source(s)
PM1	A provider can initiate, save, and apply to be a Medicaid provider.	42 C.F.R. §455.410(a)
PM2	A state user can view screening results from other authorized agencies (Medicare, CHIP, other related agencies) to approve provider if applicable.	42 C.F.R. §455.410(c)
PM3	A state user can verify that any provider purporting to be licensed in a state is licensed by such state and confirm that the provider's license has not expired and that there are no current limitations on the provider's license ensure valid licenses for a provider.	42 C.F.R. §455.412
PM4	The system tracks the provider enrollment period to ensure that the state initiates provider revalidation at least every five years.	42 C.F.R. §455.414
PM5	A state user (or the system, based on automated business rules) must terminate or deny a provider's enrollment upon certain conditions (refer to the specific regulatory requirements conditions in 42C.F.R.455.416).	42 C.F.R. §455.416
PM6	After deactivation, a provider seeking reactivation must be re-screened by the state and submit payment of associated application fees before their enrollment is reactivated.	42 C.F.R. §455.420
PM7	A provider can appeal a termination or denial decision~~,~~ and a state user can monitor the appeal process and resolution including nursing homes and ICFs/IID.	42 C.F.R. §455.422
PM8	A state user can manage information for mandatory pre-enrollment and post-enrollment site visits conducted on a provider in a moderate or high-risk category.	42 C.F.R. §455.432(a)
PM9	A state user can view the status of criminal background check~~s~~, fingerprinting, and site visits for a provider as required based on their risk level and state law.	42 C.F.R. §455.434
PM10	The system checks appropriate databases to confirm a provider's identity and exclusion status for enrollment and reenrollment and conducts routine checks using federal databases including: Social Security Administration's Death Master File, the National Plan and Provider Enumeration System (NPPES), the List of Excluded Individuals/Entities (LEIE), and the Excluded Parties List System (EPLS). Authorized users can view the results of the data matches as needed.	42 C.F.R. §455.436

Reference #	Outcome	Source(s)
PM 11	A state user can assign and screen all applications by a risk categorization of limited, moderate, or high for a provider at the time of new application, re-enrollment, or re-validation of enrollment. A state user can adjust a provider's risk level due to payment suspension or moratorium.	42 C.F.R. §455.450
PM 12	The system can collect application fees. A state user ensures any applicable application fee is collected before executing a provider agreement.	42 C.F.R. §455.460
PM 13	A state user can set CMS and state-imposed temporary moratoria on new providers or provider types in six-month increments.	42 C.F.R. §455.470
PM 14	A state user can determine network adequacy based upon federal regulations and state plan.	42 C.F.R. §438.68
PM 15	A state user, and/or the system, can send and receive provider sanction and termination information shared from other states and Medicare to determine continued enrollment for providers.	42 C.F.R. §455.416(c)
PM 16	The system can generate relevant notices or communications to providers to include, but not limited to, application status, requests for additional information, re-enrollment termination, investigations of fraud, suspension of payment in cases of fraud.	42 C.F.R. §455.23
PM 17	A state user can report required information about fraud and abuse to the appropriate officials.	42 C.F.R. §455.17
PM 18	The system, or a state user, can suspend payment to providers in cases of fraud.	42 C.F.R. §455.23
PM 19	A state user can view provider agreements and disclosures as required by federal and state regulations.	42 C.F.R. §455.104 42 C.F.R. §455.105 42 C.F.R. §455.106 42 C.F.R. §455.107
PM 20	A state user can view information from a managed care plan describing changes in a network provider's circumstances that may affect the provider's eligibility to participate in Medicaid, including termination of the provider agreement.	42 C.F.R. §438.608(a)
PM 21	A beneficiary can view and search a provider directory.	42 C.F.R. §438.10(h)

Table B-11: Third Party Liability (TPL) Outcomes

Reference #	Outcome	Source(s)
TPL1	The system does the following: • Records third parties, • Determines the liability of third parties, • Avoids payment of third-party claims, • Recovers reimbursement from third parties after Medicaid claims payment, and • Records information and actions related to the plan.	42 C.F.R. §433.138(k)(2)(i)
TPL2	The system records other health insurance information at the time of application or renewal for Medicaid eligibility that would be useful in identifying legally liable third-party resources.	Section 1902(a)(25) of the Act 42 C.F.R. §433.136 42 C.F.R. §433.137 42 C.F.R. §433.138
TPL3	The system uses electronic exchange state wage information collection agency The system(s) regularly updates the member file with any third-party liability information, how long it is valid, and for what services, through regular automated checks with these databases.	42 C.F.R. §433.138(d) and (f) 42 C.F.R. §435.4 State Plan
TPL4	The system rejects and returns to the provider for a determination of the amount of liability for all claims for which the probable existence of third-party liability is established at the time the claim is filed.	42 C.F.R. §433.139(b)
TPL5	For claims identified with a third-party liability and designated as “mandatory pay and chase,” the system makes appropriate payments and identifies such claims for future recovery. (Examples include preventive pediatric services provided to children, or medical child support from an absent parent.)	Section 1902(a)(25) of the Act 42 C.F.R. §433.139(b)(3)(ii)
TPL6	The system(s) supports providing up to 100 days to pay claims related to medical support enforcement, preventive pediatric services, labor and delivery, and postpartum care that are subject to "pay and chase." If a state cannot differentiate the costs for prenatal services from labor and delivery on the claim, it will have to cost avoid the entire claim.	Bipartisan Budget Act of 2018, Sec. 53102 Section 1902(a)(25) of the Act CMCS Informational Bulletin (CIB) November 14, 2019 (pg. 2)
TPL7	The system identifies paid claims that contain diagnosis codes indicative of trauma, injury, poisoning, and other consequences of external causes on a routine and timely basis for the purposes of determining legal liability of third parties.	42 C.F.R. §433.138(e) and (f)

Reference #	Outcome	Source(s)
TPL8	The system identifies probable TPL within 60 days after the end of the month in which payment has been made (unless there is an approved waiver to not recoup funds).	42 C.F.R. §433.139(d)
TPL9	The system can generate reports on data exchanges and trauma codes so that the state can evaluate its TPL identification process.	42 C.F.R. §433.138(j)
TPL10	The system enables the agency to seek reimbursement from a liable third party on all claims for which it is cost effective.	42 C.F.R. §433.139(f)
TPL11	As determined by the state policies, system(s) enables the state to manage and oversee TPL recoveries made by its MCOs.	COB/TPL Training and Handbook- 2020 (pg. 53-55)
TPL12	Before requesting information from or releasing information to other agencies to identify legally liable third-party resources, state must execute data exchange agreements with those agencies.	42 C.F.R. §433.138(h)
TPL13	The system tracks TPL reimbursements received so that the state can reimburse the Federal Government in accordance with the state's FMAP.	42 C.F.R. §433.140(c)

Table B-12: Program Integrity (PI)

Reference #	Outcome	Source(s)
CP2	The system performs comprehensive validation of claims and claims adjustments, including validity of services.	42 C.F.R. §431.052 42 C.F.R. §431.055 42 C.F.R. §447.26 42 C.F.R. §447.45(f) 45 C.F.R. §162.1002 SMD Letter 10-017 SMM Part 11 Section 11300
FM5	The system accurately tallies recoupments by tracking repayments and amounts outstanding for individual transactions and in aggregate for a provider.	42 C.F.R. §447
PBM9	The system supports the identification of patterns of fraud, abuse, gross overuse, or inappropriate or medically unnecessary care, or prescribing or billing practices indicating abuse or excessive utilization among physicians, pharmacists and individuals receiving benefits by enabling the collection of pharmacy data to be used in retrospective drug utilization reviews.	Section 1927 (g) of the SSA 42 C.F.R. §456.703 42 C.F.R. §456.705(b) 42 C.F.R. 456.709

Reference #	Outcome	Source(s)
PI1	System can check member record to ensure the member on the claim was enrolled in the Medicaid program and the benefit was covered at the time of service. Membership enrollment records the system is checking against are updated daily. **Applicable to CP*	42 C.F.R. §455.1(a)
PI2	System provides a method for identifying suspected inappropriate services and incorrect billing. **Applicable to CP, E&E, MM*	42 C.F.R. §455.13
PI3	System can verify with beneficiaries whether services billed by providers were received.	42 C.F.R. §455.20
PI4	System can suspend Medicaid payments in whole or in part to providers for whom the agency has determined there is a credible allegation of fraud and is conducting an investigation and other activities, including provide notice of suspension; referrals to MFCU; and documentation and record retention.	42 C.F.R. §455.23(a-g)
PI5	System can perform provider lock-in for identified members responsible for fraudulent activity, or that have utilized services in excess of what is medically necessary (as defined by state guidelines), and can send notice to the impacted member and the appropriate provider. **Applicable to PM*	42 C.F.R. §431.54(f)
PI6	System can recover improper payments by: (a) Tracking repayments and outstanding amounts due at an individual transaction level as well as aggregating by provider, time period (b) Supporting electronic transfer back to the state (c) Temporarily limiting future payments to provider(s) who have an outstanding recovery balance.	42 C.F.R. §447 42 C.F.R. §431.1002 42 C.F.R. §433.300-322
PI7	System can complete the required independent certified audit of Disproportionate Share Hospital (DSH) payments for each Medicaid State Plan rate year using payment and utilization information.	42 C.F.R. §455.304(d)
PI8	System can reject claims for items or services that were ordered or referred that do not contain a National Provider Identifier. **Applicable to CP*	42 C.F.R. §455.440

Reference #	Outcome	Source(s)
PI9	System can support activities conducted by Medicaid RACs can including review all claims submitted by providers of items or services for which payment has been made to identify underpayments and overpayments and recoup overpayments as necessary.	42 C.F.R. §455.506
PI10	System can refer all cases of suspected provider fraud to the state's Medicaid Fraud Unit and provide access to Case Tracking as applicable.	42 C.F.R. §455.21(a)
PI11	System can sample and review active cases, including negative cases, to determine eligibility errors in accordance with the state's MEQC pilot planning document.	42 C.F.R. §431.814(b)
PI12	System can submit following information to CMS for among other purposes, estimating improper payments in Medicaid and CHIP, that include, but are not limited to— (1) Adjudicated fee-for-service or managed care claims information, or both, on a quarterly basis, from the review year; (2) Upon request from CMS, provider contact information that has been verified by the state as current; (3) All medical, eligibility, and other related policies in effect, and any quarterly policy updates; (4) Current managed care contracts, rate information, and any quarterly updates applicable to the review year; (5) Data processing systems manuals; (6) Repricing information for claims that are determined during the review to have been improperly paid; (7) Information on claims that were selected as part of the sample, but changed in substance after selection, for example, successful provider appeals; (8) Adjustments made within 60 days of the adjudication dates for the original claims or line items, with sufficient information to indicate the nature of the adjustments and to match the adjustments to the original claims or line items; (9) Case documentation to support the eligibility review, as requested by CMS; (10) A corrective action plan for purposes of reducing erroneous payments in FFS, managed care, and eligibility; and (11) Other information that the Secretary determines is necessary for these purposes.	42 C.F.R. §431.970

Reference #	Outcome	Source(s)
PM11	System can assign and screen all applications by a risk categorization of limited, moderate, or high for a provider at the time of new application, re-enrollment, or re-validation of enrollment. A state user can adjust a provider's risk level due to payment suspension or moratorium.	42 C.F.R. §455.450
PM17	A state user can report required information about fraud and abuse to the appropriate officials.	42 C.F.R. §455.17
PM18	The system can suspend payment to providers in cases of fraud.	42 C.F.R. §455.23

B-13: Health Information Exchange (HIE)

Please note that, although there are not CMS-required outcomes for Health Information Exchange (HIE) modules, all other Streamlined Modular Certification requirements apply (e.g., the CEF, state-specific outcomes).

APPENDIX C: REQUIRED ARTIFACTS LIST

The following table contains the list of artifacts required for an Operational Readiness Review (ORR) and Certification Review (CR). Minimum requirements for each document are given, but this not an exhaustive list of what typically is included in each artifact. States are encouraged to add elements, as appropriate.

Topic	Document/ Artifact	Minimum Required Content and Notes	Required at ORR, CR, or Both
Entry Criteria for CR	**Official Certification Request Letter**	• The date the system became the system of record. • A copy of the state's letter to the vendor, contractor or state development team accepting the system/modules(s). • The effective date for which the state is requesting certification approval. • A proposed timeframe for the CR. • A declaration that the state's system meets all the requirements of law and regulation, including 42 C.F.R. §433.117 for all periods for which the 75 percent FFP is being claimed. • The state maintains monthly production submissions of Transformed Medicaid Statistical Information System (T-MSIS) files. (States will be deemed out of compliance with timeliness requirements if T-MSIS files are submitted later than one month after the T-MSIS reporting period.) • The state maintains complete and accurate historical T-MSIS data for program evaluation and the continuous improvement of business operations. • The state can demonstrate that data quality issues are meeting the targets for Outcomes Based Assessment (OBA) critical priority data quality checks, high priority data quality checks, and the expenditure data content category. The state should also demonstrate they are working in good faith to resolve such issues. Generally, CMS will consider the state out of compliance with T-MSIS requirements if it is not meeting the targets for OBA criteria in critical priority data quality checks, high priority data quality checks, and the expenditure data content category and/or the state is not working in good faith to resolve any identified data quality issues. • The state meets all requirements outlined in the T-MSIS Reporting - Standard Operating Procedures (SOP) for any Large System Enhancements (LSEs) affecting T-MSIS reporting. • Is ready for CMS certification, based on the system's performance in demonstrating achievement of outcomes.	Submitted to begin the CR process
Entry Criteria for CR	**System Acceptance Letter**	A copy of the state's acceptance letter addressed to the system developer indicating that the system or module was accepted as fully operational at least six months prior to the requested certification review date.	Submitted to begin the CR process

Topic	Document/ Artifact	Minimum Required Content and Notes	Required at ORR, CR, or Both
Project Management	**Monthly Project Status Reports**	Indicators of Project Health, which are: • **Roadmap** - A product roadmap identifying current, planned, and future functionality and milestones. • **Progress Tracking** - A regular report measuring development progress and progress towards achieving outcomes. • **User Feedback** - A reporting showing how user feedback is regularly incorporated into development. • **Defect and Risk List** - Known defects and risks that may cause delays and any mitigations or workarounds. • **Product Demos** - Demo of functionality/features, or regular report of code/feature releases. • **Testing Process** - A documented testing process aligned with the ***Testing Guidance Framework***.	Both
Technical	**Master Test Plan and Testing Results**	• State testing should be informed by the ***Testing Guidance Framework*** document, which offers specific MES testing expectations and recommendations. • Test results should not only validate the iterative delivery of system functionality, but also confirm that the system will produce metrics associated with outcomes. • Testing should be as automated and self-documenting as possible (e.g., continuous unit testing). • Test results should be mapped to functionality, with an acceptance testing report for each user story/use case.	Both
Technical	**Deployment Plan**	• Description of the release and deployment of a new/updated module agreed upon by all stakeholders. • Compatibility between all of the related assets and service components within each release package is verified. • Via the configuration management process in place, verify that the integrity of release packages and their constituent components are maintained throughout the transition activities. • Define how release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out, if appropriate. • Define how deviations, risks, and issues related to the new or updated module are recorded and how corrective actions are ensured. • Define how the transfer of knowledge will occur to enable end users to optimize their use of the new/updated module to support their business activities. • Define the transfer of skills and knowledge to operations staff to effectively and efficiently deliver, support, and maintain the new/updated module according to the documented Service Level Agreements (SLAs).	ORR

Topic	Document/ Artifact	Minimum Required Content and Notes	Required at ORR, CR, or Both
Technical	**Defect and Risk List**	• Current defect list, with frequency, severity (inclusive of all critical and high defects), and associated implementation timelines. • Defect entries should include information about the operational impact. • Risks should be accompanied by a mitigation/resolution or a risk acceptance statement.	Both
Technical	**Independent Security Audit**	The independent, third-party security and privacy controls assessment report that covers compliance with the following: • NIST SP 800-171 and/or NIST SP 800-53 standards and all relevant controls in HIPAA; • aligning Health Care Industry Security Approaches pursuant to Cybersecurity Act of 2015, Section 405(d); and • the Open Web Application Security Project Top 10. Risks should be identified using NIST SP 800-30 Revision 1. The third-party audit should include, but need not be limited to, a penetration test, a review of all HIPAA compliance areas: user access control; information disclosure; audit trail; data transfers; and information on correct data use (i.e., role-based testing of use). The audit should cover adequate audit trails and logs (e.g., ID, access level, action performed, etc.). The audit should also cover encryption of data at rest, in audit logs, and in transit between workstations and mobile devices (where applicable), to external locations and to offline storage.	ORR

APPENDIX D: FRAMEWORK FOR THE INDEPENDENT THIRD-PARTY SECURITY AND PRIVACY ASSESSMENT GUIDELINES FOR MEDICAID ENTERPRISE SYSTEMS

Table of Contents

List of Tables

1. Introduction

The state Medicaid Enterprise System (MES) is the custodian of sensitive information, such as Personally Identifiable Information (PII) and Protected Health Information (PHI), for millions of individuals receiving coverage through Medicaid and the Children's Health Insurance Program. The state and its business partners share the responsibility for ensuring the protection of this sensitive information. States and their respective business partners must demonstrate continuous monitoring and regular security and privacy control testing through an independent security and privacy assessment.

This guidance document provides an overview of the independent security and privacy assessment requirements. It contains guidelines for both cloud-based and non-cloud-based environments. The state can tailor guidelines based on the solution's implementation. This guidance is applicable for the states that work directly with a third-party assessment vendor or a MES solution vendor working with a third-party assessment vendor.

1.1 Requirements Background

Pursuant to the Health Insurance Portability and Accountability Act (HIPAA) and implementing regulations at 45 Code of Federal Regulations (C.F.R.) §164.308(a)(1)(ii)(A), conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications of HIPAA. Therefore, a risk analysis is foundational and must be completed to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards of PHI/PII. Furthermore, the National Institute of Standards and Technology (NIST), Security Assessments Control, CA-2, requires an independent assessment of all applicable security and privacy controls. States should have a fully completed and implemented System Security/Privacy Plan (SSP) before starting the security and privacy assessment. The Centers for Medicare & Medicaid Services (CMS) highly recommends that an independent third-party assessor conduct the assessment.

If the state has adopted a framework similar or complementary to NIST that supports the HIPAA requirements, then the state may use that framework to do risk analysis.

If NIST is not the core framework of the third-party assessor, then the third-party assessor needs to provide a translation or crosswalk of the supported framework to the NIST controls.

1.2 Purpose

This guidance document provides an overview of the independent security and privacy assessment requirements through the following objectives:

- Define the independent third-party assessor (Section 2).
- Explain the scope of the security and privacy control assessment and provide assessment planning considerations (Section 3).
- Provide a basic security and privacy control assessment methodology (Section 4).
- Summarize security and privacy assessment reporting (Section 5).

This document is not intended to provide detailed guidance for assessment planning and performance, nor for state planning and action to address assessment findings.

2. Independent Third-Party Security and Privacy Assessor

Pursuant to 45 C.F.R. §95.621(f) and consistent with State Medicaid Directors Letter #06-022,[6] CMS requires that state agencies employ assessors or assessment teams to conduct periodic security and privacy control assessments of the MES environment. The assessor's role is to provide an independent assessment of the effectiveness of implementations of security and privacy safeguards for the MES environment and to maintain the integrity of the assessment process. Alternatively, states can require vendors to have their own independent third-party assessment and provide assessment results.

2.1 Assessor Independence and Objectivity

An assessor must be free from any real or perceived conflicts of interest, including being free from personal, external, and organizational impairments to independence, or the appearance of such impairments to independence. An assessor is considered independent if there is no perceived or actual conflict of interest involving the developmental, operational, financial, and/or management chain associated with the system and the determination of security and privacy control effectiveness.

NIST Special Publication (SP) 800-39, *Managing Information Security Risk,*[7] states that:

> "Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision."

2.2 Assessor Qualifications

Experience and competencies are important factors in selecting an assessor. CMS recommends that the MES assessor possess a combination of privacy and security experience and relevant assessment certifications. Examples of acceptable privacy and security experience may include, but are not limited to:

- Reviewing compliance with HIPAA security standards.
- Reviewing compliance with the most current NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, or the most current NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.[8]
- Reviewing compliance with the Minimal Acceptable Risk Standards for Exchange.
- Reviewing compliance with the Federal Information Security Management Act.
- Participating in the Federal Risk and Authorization Management Program (FedRAMP)-certified third-party assessment organization.
- Reviewing compliance with the Statement on Standards for Attestation Engagements 16.
- Experience assessing the implementation of the Center for Internet Security (CIS) benchmarks.

---

[6] Available at: https://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/SMD092006.pdf
[7] Available at: https://csrc.nist.gov/publications/detail/sp/800-39/final
[8] If a framework other than NIST is used, then provide that framework and a crosswalk of the framework to the NIST controls.

- Reviewing compliance with the Open Web Application Security Project (OWASP).

The assessor organizations should have relevant security and privacy accreditations, and the assessor's team leads should have relevant security and privacy certifications. Examples of relevant auditing certifications are:

- Certified Information Privacy Professional
- Certified Information Privacy Manager
- Certified Information Systems Security Professional
- Fellow of Information Privacy
- HealthCare Information Security and Privacy Practitioner
- Certified Internal Auditor
- Certified Risk Management Professional
- Certified Information Systems Auditor
- Certified Government Auditing Professional
- Certified Expert HIPAA Professional

2.3 Assessor Options

CMS strongly recommends the use of an experienced third-party security and privacy assessor. However, internal state staff may be leveraged, provided they have appropriate qualifications to evaluate the implementation of security and privacy controls. The internal state staff must be familiar with HIPAA regulations, NIST standards, and other applicable federal privacy and cybersecurity regulations and guidance. They must also meet the assessor independence, objectivity, and qualifications documented in Sections 2.1 and 2.2. Furthermore, they must be capable of performing penetration testing and vulnerability scans.

3. Assessment Scope and Planning

3.1 Scope of the Independent Security and Privacy Control Assessment

The purpose of a Security Control Assessment (SCA) is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the application or system. The SCA also identifies areas of risk that require the state's attention and remediation. The independently conducted SCA provides an understanding of the following:

- The MES application or system's compliance with the state security and privacy control requirements.
- The underlying infrastructure's security posture.
- Any application and/or system security, data security, and privacy vulnerabilities to be remediated to improve the MES's security and privacy posture.
- The state's adherence to its security and privacy program, policies, and guidance.

3.2 Vulnerabilities and Testing Scenarios

Given the sensitivity of data processed in the MES and the high threat of the web environment, it is critically important that the security of web applications deployed meet the present-day known security

attack vectors and situations. OWASP keeps an up-to-date list that identifies such attacks and situations.[9] In addition to the mandated security and privacy controls, the independent SCA requires vulnerability assessments to determine vulnerabilities associated with known attacks and situations obtained from the current OWASP Top 10 – *The Ten Most Critical Web Application Security Risks*. The assessment should adjust the SCA scope to address the current OWASP list of vulnerabilities. The state should regularly review the following list to determine the current vulnerabilities in the OWASP Top 10, including, but not limited to:

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

3.3 Assessment of Critical Security Controls

Test scenarios should adequately assess the implementation status of critical security controls identified by the Center for Internet Security (CIS).[10] The CIS controls are mapped to the NIST controls. The testing scenario information for each CIS control is available at the CIS site. The main testing points identified by the CIS are incorporated into the SCA scope, corresponding Security and Privacy Controls Assessment Test Plan (SAP), and testing criteria.

CIS benchmarks are specific to environmental components such as server operating system hardening, networking configurations, or cloud service implementations. Where benchmarks exist, they should be applied to the system configurations.

3.4 Assessment Planning

The state is encouraged to develop an assessment strategy and procedure that provides a standardized approach for planning and resourcing the SCA of its applications, systems, and underlying components. The state is responsible for ensuring that each SCA has:

- Budget and assigned resources suitable for completing the assessment
- Clear objectives and constraints
- Well-defined roles and responsibilities
- Scheduling that includes defined events and deliverables

During planning for the SCA, the state develops a scope statement that is dependent on, but not limited to, the following factors:

- Application or system boundaries

[9] Available at: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
[10] CIS Top 20 Critical Controls, available at: https://www.cisecurity.org/controls/.

- Known business and system risks associated with the application or system
- Dependence of the application or system on any hierarchical structure
- Current application or system development phase
- Documented security and privacy control requirements

The assessor's SCA contract statement of work should include requirements to provide support to clarify findings and make corrective action recommendations after the assessment. The contract terms should also specify that all assessor staff must execute appropriate agreements such as Non-Disclosure Agreement, Memorandum of Understanding, or HIPAA Business Associate Agreement for the protection of sensitive data before accessing any information related to the security and privacy of the application or system. Requests to access information should only be considered based on a demonstration of a valid need-to-know level, ***not*** a position, title, level of investigation, or position sensitivity level.

4. Security and Privacy Control Assessment Methodology

The SCA methodology described in this guidance originates from the standard CMS methodology used in the assessment of all CMS internal and business partner applications or systems.

Assessment procedures for testing each security and privacy control should be consistent with the methodology documented in the most current version of NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*.[11] The assessor should prepare a detailed assessment plan using these security and privacy control assessment procedures, the main testing points for the CIS critical controls, and detailed directions for addressing the penetration testing procedures for the OWASP Top 10 vulnerabilities. The assessor should modify or supplement the procedures to evaluate the application's or system's vulnerability to different types of threats, including those from insiders, the Internet, or the network. The assessment methods should include examination of documentation, logs and configurations, interviews of personnel, and testing of technical controls.

Control assessment procedures and associated test results provide information to identify the following:

- Application or system vulnerabilities, the associated business and system risks, and potential impact
- Weaknesses in the configuration management process, such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system
- State and/or federal policies not followed
- Major documentation omissions and/or discrepancies

4.1 Security and Privacy Control Technical Testing

To conduct security technical testing, the state grants assessor staff user access to the application or system. The state system administrator establishes application-specific user accounts for the assessor that reflect the different user types and roles. Through this access and these accounts, the assessor can perform a thorough assessment of the application or system and test application and system security controls that might otherwise not be tested. The assessor should not be given a user account with a role that would allow access to PHI/PII in any application or database.

[11] Available at: https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final.

The assessor should attempt to expose vulnerabilities associated with gaining unauthorized access to the application or system resources by selecting and employing tools and techniques that simulate vulnerabilities, such as buffer overflows and password compromises. The assessor must use caution to ensure against any inadvertent alteration of important settings that may disable or degrade essential security or business functions. Because many automated testing utilities mimic signs of attack and/or exploit vulnerabilities, the assessor must identify in the SAP all proposed tools that pose a risk to the computing environment.

The MES solution can be tested in a test environment or a pre-production environment provided these environments host an instance of the production operational environment. The testing or pre-production environments should mirror the production environment to generate an accurate response. Any deviations in these environments used for testing should properly documented. States or vendors should certify and attest that all system vulnerabilities found as a result of security and privacy assessment performed in a test or a pre-production environment will also be mitigated in the production environment.

4.2 Network and Component Scanning

To gain an understanding of a network and component infrastructure security posture, the SCA includes network-based infrastructure scans, database scans, web application scans, and penetration tests for all in-scope components, applications, and systems. This scope provides a basis for determining the extent to which the security controls implemented within the network meet security control requirements. The assessor evaluates the results of these scans in conjunction with the configuration assessment.

4.3 Configuration Assessment

The configuration assessment provides the assessor with another mechanism for determining if the state's security requirements are implemented correctly in the application or system, or if the system environmental components are implemented correctly within the boundary of the application or system. Performing the configuration assessment requires the assessor to:

- Review the implemented configurations for each component against the state's security and privacy requirements.
- Review access to the system and databases for default user accounts.
- Test firewalls, routers, systems, and databases for default configurations and user accounts.
- Review firewall access control rules against the state's security requirements.
- Determine consistency of system configuration with the state's documented configuration standards

4.4 Documentation Review

The assessor should review all security and privacy documentation for completeness and accuracy and gain the necessary understanding to determine the security and privacy posture of the application or system. Through this process, the assessor develops insight into the documented security and privacy controls in place to effectively assess whether all controls are implemented as described. The documentation review augments all testing – It is an essential element for evaluating compliance of the documented controls versus the actual implementation as revealed during technical testing, scanning, configuration assessment, and personnel interviews.

For example, if the specified control stipulates that the password length for the system must be eight characters, the assessor must review the state's password policy or the SSP to verify compliance with this requirement. During the technical configuration assessment, the assessor confirms that passwords are configured as stated in the state's documentation. Table 1 identifies examples of core security documentation for review.

Table 1. Core Security and Privacy Documentation

NIST/State Control Family	NIST/State Control Number	Document Name
Planning (PL)	PL-2: System Security and Privacy Plan (SSP)	System Security and Privacy Plan (SSP)
Configuration Management (CM)	CM-9: Configuration Management Plan	Configuration Management Plan (CMP)
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing and Exercises	CP Test Plan and Results
Incident Response (IR)	IR-8: Incident Response Plan	Incident Response Plan (IRP)
Incident Response (IR)	IR-3: Incident Response Testing and Exercises	IRP Test Plan
Awareness and Training (AT)	AT-3: Security Training	Security Awareness Training Plan
Awareness and Training (AT)	AT-4: Security Training	Training Records
Security and Assessment Authorization (CA)	CA-3: System Interconnections	Interconnection Security Agreements (ISA)
Risk Assessment (RA)	RA-3: Risk Assessment	Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	Privacy Impact Assessment (PIA) or other privacy documents
Authority and Purpose (AP)	AP-2: Purpose Specification	Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PHI/PII and Privacy Act Statements
Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program	Governance documents and privacy policy
Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment	Documentation describing the organization's privacy risk assessment process, documentation of privacy risk assessments performed by the organization

4.5 Personnel Interviews

The assessor conducts personnel interviews to validate the implementation of security and privacy controls, confirm that state and/or MES solution vendor staff understand and follow documented control implementations, and verify the appropriate distribution of updated documentation to staff. The assessor interviews business, information technology (IT), and support personnel to ensure effective

implementation of operational and managerial security and privacy controls across all support areas. The assessor will customize interview questions to focus on control assessment procedures applicable to individual roles and responsibilities and ensure that state staff are properly implementing and/or executing security and privacy controls.

The SCA test plan identifies the designated state and/or MES solution vendor subject matter experts (SMEs) to interview. These SMEs should have specific knowledge of overall security and privacy requirements and a detailed understanding of the application or system operational functions. The staff selected for conducting interviews may have the following roles:

- Business Owner(s)
- Application Developer
- Configuration Manager
- Contingency Planning Manager
- Database Administrator
- Data Center Manager
- Facilities Manager
- Firewall Administrator
- Human Resources Manager
- Information System Security Officer
- Privacy Program Manager
- Privacy Officer
- Media Custodian
- Network Administrator
- Program Manager
- System Administrator(s)
- System Owner
- Training Manager

Although the initial identification of interviewees is determined when the SAP is prepared, additional staff may be identified for interviewing during the SCA process.

4.6 Penetration Testing

At a minimum, penetration testing includes the tests found in Section 3.2 (based on the OWASP Top 10). The Security and Privacy Controls Assessment Test Plan should document the tools, methods, and processes for penetration testing. The test plan should clearly account for and coordinate any special requirements or permissions for penetration testing during the SCA.

A penetration test is a comprehensive way of testing an organization's cybersecurity vulnerabilities and compliance with the adopted security and privacy standards. Penetration testing views the network, application, device, and physical security through the eyes of both a malicious actor and an experienced cybersecurity expert to discover weaknesses and identify areas where the security posture needs improvement, and subsequently, ways to remediate the discovered vulnerabilities.

5. Security and Privacy Assessment Reporting

At the completion of the assessment, the assessor provides a Security and Privacy Assessment Report (SAR) to the state's Business Owner, who is then responsible for providing the report to CMS. The SAR's structure and content (as described in the following subsection) must be consistent with the assessment objectives. The SAR allows the assessor to communicate the assessment results to several audience levels, ranging from executives to technical staff.

The SAR is not a living document; findings should not be added to or removed from the SAR.

5.1 SAR Content

The SAR content may include, but is not limited to, the following information:

- System Overview
- Executive Summary Report
- Detailed Findings Report
- Scan Results
  - Infrastructure Scan
  - Database Scan
  - Web Applications Scan
- Penetration Test Report
- Penetration Test and Scan Results Summary

The SAR presents the results of all testing performed, including technical testing, scans, configuration assessment, documentation review, personnel interviews, and penetration testing. Results from multiple testing sources may be consolidated in one finding, if results are closely related. The findings of the assessment should be annotated in detail with the remediation recommendations for the weaknesses and deficiencies found in the system security and privacy controls implementation. To reduce the risks posed to this important healthcare service and to protect the sensitive information of the citizens who use this service, the assessment team must assign business and system risk levels to each specific finding. The assignment of these risk levels should follow the methodology outlined in NIST SP 800-30 Rev. 1, Appendices G, H, and I.[12]

The SAR structure should allow the independent third-party assessor to communicate the security and privacy assessment results to several targeted audience levels, ranging from executives to technical staff. A sample SAR can be modeled after one used by FedRAMP.[13]

[12] NIST 800-30 Rev.1, Appendices G, H, and I. Available at: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.
[13] FedRAMP SAR Template. Available at: https://www.fedramp.gov/templates/.

6. Incident and Breach Reporting Procedures

CMS considers a security or privacy incident[14] or breach[15] of beneficiary PHI/ PII to be a serious matter. Therefore, state agencies which are found to be out of compliance with the privacy or security requirements outlined in this guidance can expect suspension or denial of FFP for their information systems and may be subject to other penalties under federal and state laws and regulations.

Under HIPAA standards, states must require that contractors and other entities performing claims processing, third-party (or other payment or reimbursement) services on their behalf protect PHI/PII privacy and security through business associate agreements. In so doing, states should ensure that their business associates update their procedures as necessitated by environmental or operational changes affecting security and privacy safeguards. The HIPAA Breach Notification Rule, 45 C.F.R. §164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, pursuant to Section 13407 of the HITECH Act.

Visit the HHS HIPAA Breach Notification Rule website for more information and guidance on the breach reporting requirements.[16] In addition to the above HIPAA requirements, the state, in turn, should immediately report a security or privacy incident or breach, whether discovered by its own staff or reported by a contractor, to the CMS State Officer and CMS IT Service Desk at cms_it_service_desk@cms.hhs.gov. If a state is unable to report breaches to the CMS IT Service Desk via email, the state can contact the CMS IT Service Desk by phone at (800) 562-1963 or (410) 786-2580.

7. Summary

All organizations should either perform an internal state risk assessment or engage an industry-recognized security and privacy assessment organization to conduct an external third-party risk assessment (CMS preferred method) of the MES implementation in order to identify and address security and privacy vulnerabilities. Information security and privacy safeguards and continuous monitoring are dynamic processes that must be managed effectively and proactively to support organizational risk management decisions. Independent security and privacy assessment provides a mechanism for the organization to identify and respond to new vulnerabilities, evolving threats, and a constantly changing enterprise architecture and operational environment, which can feature changes in hardware or software, as well as risks from the creation, collection, disclosure, access, maintenance, storage, and use of data. Through ongoing assessment and authorization, organizations can detect

---

[14] OMB Memorandum M-17-12 defines “incident” or “security incident” as an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (OMB Memorandum M-17-12, *Preparing for or Responding to A Breach of Personally Identifiable Information,* January 3, 2017. Located at: http://www.osec.doc.gov/opog/privacy/Memorandums/OMB_M-17-12.pdf.

[15] OMB Memorandum M-17-12 defines “breach” as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information for anything other than an authorized purpose.

[16] Located at: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

changes to the security and privacy posture of an IT system, which is essential to making well-informed, risk-based decisions about the system within the MES.

APPENDIX E: INTAKE FORM TEMPLATE

The Intake Form Template is used throughout the Streamlined Modular Certification process to track information about a state MES project for certification. It is tailored for each state project. States will fill out the ***Intake Form Template*** by entering the CMS-required outcomes that document compliance with regulations applicable to their project, their state-specific outcomes, and the metrics used to show that the project is achieving its outcomes on a continuous basis.

The outcomes and metrics included in Intake Form Template information should match what is included in the APD. As the state progresses with the project, the state along with their CMS State Officer will identify and document in the Intake Form Template, the evidence to be provided to demonstrate that outcomes have been achieved. As the ORR approaches, CMS and the state will finalize the specific evidence to be provided by the state. The detailed results of the ORR evaluation and the CR are also documented in the Intake Form Template. Using a single Intake Form Template to record information for the ORR and CR allows CMS to maintain an audit record for all certification activities.

Please see the CMS Certification GitHub Repository for the Intake Form Template.