COSMOS
Navigate the Compliance Universe

Compliance Today - January 2018
Certifying Medicaid program data, Part 2: Pre-data submission diligence

By Jay Davis, JD, CHC, CHPC, CCEP, CIPP/US, CIPM

Jay Davis (jaydavis@jaydavislegal.com) is an Attorney focusing in privacy, ethics, compliance, and healthcare, practicing in the greater Los Angeles area.

- linkedin.com/in/jaydavislosangeles

Part 1 of this article appeared in the December 2017 issue of Compliance Today.

Part 1 of this article presented an overview of the recently overhauled Medicaid managed care program regulations and the need to conduct pre-submission diligence to validate the accuracy, completeness, and truthfulness of the certified data submissions. To help meet the new requirements, a data validation and testing process should be integrated into existing managed care compliance programs.

Part 2 presents two examples of implementing a pre-submission data diligent review, testing, and validation process. The examples illustrate how a Compliance department-driven, pre-submission review process can promote Medicaid program compliance and integrity, lessen regulatory sanctions, and protect against potential claims under the False Claims Act.

Pre-review diligence examples

Consider two examples of how a diligent data review and testing process may be used to promote Medicaid program compliance and integrity, lessen regulatory sanctions, and help build a protective moat against potential claims under the False Claims Act. The first example involves a network adequacy data submission and the second pertains to an encounter data submission. These data submissions are essential to state monitoring and administration of major Medicaid program requirements and activities and are subject to close regulatory scrutiny by the state.

Network adequacy data submission

Medicaid managed care entities (MMCEs) must demonstrate to the state that they have and maintain an adequate provider network to meet network adequacy requirements under the final rule and state regulations. An MMCE-certified network adequacy data submission relates to key Medicaid program requirements that services be available and accessible to enrollees. Inaccurate and deficient data submissions may flow from inadequate data testing and validation processes and result in state-imposed corrective action and potential monetary sanctions.

Primary considerations in network adequacy submissions will likely be the accuracy of participating provider contact information (e.g., provider directory information), satisfying state time-and-distance travel requirements, provider appointment availability, and provider availability/capacity to accept or service enrollees to assure enrollee access to care. The provider relations function may have primary responsibility for assembling a network adequacy data submission. MMCE practices will vary, and data compilation may be performed by other internal operational functions or a third-party vendor.

The Compliance department should establish a diligent-review monitoring and audit protocol for testing and validating the accuracy and completeness of the submission before the data is certified. Compliance might draw a sample or monitor and audit internal or external sampling of provider network adequacy data submissions to confirm the accuracy and completeness of providers' contact information, provider staffing at service sites, appointment timeframes, and the availability/capacity of providers to service enrollees. A better practice would be to establish regular intervals for the review and testing process. This establishes a pattern of reasonable review diligence and demonstrates to regulators that ongoing monitoring, auditing, and voluntary corrective action is taken as needed.

Encounter data submission

Now consider a data submission involving encounter data. MMCEs, which are paid on per-member-per-month capitated basis by the state, must submit encounter data to the state concerning all services provided to a Medicaid enrollee. Encounter data is defined in the Medicaid managed care final rule[1] as information relating to the receipt of any item(s) or service(s) by an enrollee under a contract between a state and MMCE.[2] It includes information concerning clinical conditions diagnosed and treated and services and items delivered to enrollees to treat the conditions. The level of detail of services reported in encounter data is like that of a standard claim form.

Encounter data submissions are integral to Medicaid program administration, are subject to close regulatory scrutiny, and merit special attention in the pre-submission review and testing process. This is because encounter data plays a substantial role in Medicaid program oversight, in state rate-setting activities, and in the state's ability to obtain federal financial participation (FFP). Encounter data is a critical source of information for measuring and monitoring managed care plan quality, service utilization, and contractual compliance. This data is also used to set capitation rates and perform risk adjustment to account for differences in beneficiary health status across plans.[3] The state's submission to CMS of encounter data that the state has validated as complete and accurate is a condition for the state's receipt of FFP for expenditures the state makes under an MMCE contract. FFP may be deferred or disallowed for inaccurate or incomplete encounter data.[4] ,[5]

Sources of MMCE encounter data depend on how an MMCE contracts with network providers to provide services to enrollees. MMCEs that contract with providers on a fee-for-service basis (e.g., procedure-specific rates, fixed case rates, or per diem arrangements) will be adjudicating claims for services and will generate the encounter data. Where the MMCE contracts with network providers on a per-member-per-month capitation basis, directly contracted capitated providers and their subcontracted providers must generate and report the encounter data to the MMCE or a data aggregator.

An MMCE is dependent on receiving timely, accurate, and complete data reporting from capitated providers, which are paid prospectively and thus have less incentive to submit timely, compliant data than fee-for-service providers. The MMCE nonetheless remains responsible for obtaining compliant, accurate, and complete data from subcontractors and network providers, and their non-compliance will not excuse the MMCE's performance.[6] MMCEs must be prepared to use contractual enforcement (e.g., withholds, financial penalties, and enrollment suspension) mechanisms, as necessary, to secure compliance.