Preparing for an Audit

Magellan Behavioral Health of Pennsylvania, Inc. (Magellan) conducts audits of providers that include any combination of a Clinical Treatment Record Review in conjunction with a Claims Screening Audit, a Compliance Program Audit, and/ or a Network Audit. When a treatment record review takes place in conjunction with a claims, compliance and/ or network audit, the review is referred to as an ***Integrated Audit***. In addition to assessing that active, appropriate and high-quality clinical treatment is taking place, the purpose of these Integrated Audits is to take a more comprehensive and holistic approach to provider oversight by assessing compliance programs, billing practices, human resources aspects and other policies and procedures specific to a level of care or program. Magellan conducts the following types of Integrated Audits:

- ***Routine***- based on a statistically valid random sample selected annually from the entire network of contracted providers regardless of size and type (individual, group or organization). Programs that received a Routine Integrated Audit in the prior year are excluded from the sample.
- ***Targeted***- conducted in response to an identified concern, complaint, whistleblower, etc.
- ***Follow-up***- audit to assess implementation of a prior action plan
- ***Implementation Oversight (I/O)***- conducted on new providers who have recently joined the network.

Magellan wants to help you prepare for these Integrated Audits. We view the audit process as an opportunity for communication of expectations and enhancement of our partnership to better serve our members. The auditing process is a collaborative one and includes the provider, our County Partners and the Magellan Quality Improvement (QI), Special Investigations Unit (SIU)/ Compliance and/ or Network Departments. Reviews are typically conducted remotely; however, there are times when these reviews will be conducted on site at the provider agency. For on-site audits, the auditors will need workstations with appropriate access to the Electronic Health Records (EHR) in order to complete the audits on-site. For remote audits, we will ask providers to submit a copy of all intake documents (consents, releases, bill of rights, etc.), progress notes, treatment plans, evaluations/ assessments, crisis/safety plans and encounter forms within two business days of the scheduled review. For providers that utilize an EHR which can be accessed remotely, we ask that

log-in information is provided at least one-day prior to the scheduled review. The auditing team is typically made up of four-six participants which includes our county partners.

The specific components of an Integrated Audit includes:

- The ***Clinical Audit*** (also referred to as a treatment record review or TRR) focuses on treatment record documentation, quality of service delivery, member rights, consent to treat, releases of information, the initial evaluation, an individualized treatment plan, ongoing treatment and coordination of care. As a part of the clinical audit process, the Magellan QI Department also will assess providers on the agency's cultural competency activities.
- The ***Compliance and Claims Audit*** focuses on billing practices, compliance with state and federal regulatory requirements, provider internal claims audits, provider compliance culture; and provider compliance program components including Telehealth (e.g., policies and procedures, trainings and mandatory reporting). The Magellan SIU Department will also attempt to gain knowledge on the agency's compliance culture by conducting surveys of the staff. For providers that utilize Electronic Health Records (EHR), providers will also be asked to complete an EHR Questionnaire. The Claims portion of the audit reviews documentation, billing practices and adherence to PA Medicaid requirements. The SIU auditors will compare paid claims to the clinical documentation in the medical record as well as any Encounter Forms to ensure accuracy.
- The ***Network Audit*** includes a review of various policy and procedures within your program, staff training, supervision, a review of staff Human Resources (HR) records and the physical plant.

Audit Tools:

Audit Tools are available by contacting a representative from Magellan's Quality Improvement, SIU/ Compliance or Network Departments. Audit Tools are shared with providers electronically in advance of any Routine or I/O Audit but also can be requested at any time.

SIU Data Mining Audits:

In addition to Integrated Audits, Magellan's SIU also routinely conducts various data mining activities throughout the year. Risk-Based Claims Audits are conducted based on high volume services and/or providers to validate that the services are rendered in accordance

with State regulations and Magellan Policies. The need for an audit will be determined based on various data mining reports that are provided through the activities of Magellan's data analytics teams with input from our Compliance Committee and other stakeholders. If your provider agency is selected for a data mining review, you will receive a confirmation letter by e-mail outlining what services are being reviewed, the requested documents, the time period under review and a due date for submission. Providers will receive a letter outlining the results from the audit following the review.

SIU Investigations:

Magellan usually undertakes an investigation in response to reports of misconduct. It is a process of detailed examination to achieve certain objectives. An investigation may be conducted remotely or on-site. Prior to an a remote or announced on-site audit, you will receive notice of audit via fax, email or mail. The notice will provide details and instructions about the audit. You will not receive advance notice of an unannounced visit. SIU staff will provide you with proper identification as well as a written audit notice providing further details and instructions. During on-site audits, you will be expected to provide treatment records, personnel files, scheduling documentation, policies and procedures, or other documentation to SIU staff for review. If any of the information is maintained electronically, you will be expected to provide SIU staff with electronic access.

Please note that a lack of compliance with a request for records during any type of audit/investigation can result in:

- A Magellan Network representative contacting you.
- Retraction of payment for services not supported.
    - Any overpayment identified is referred to Magellan's Cost Containment department for recovery by refund check or future claims retractions.
- Magellan completing required reporting to a customer oversight agency.
- Placement of a subset of, or all of, a provider's claims on a pre-payment review.
- Termination from the Magellan network.