St. Clair County
Community Mental Health Authority

FY2019

Corporate Compliance Program Plan

CORPORATE COMPLIANCE PROGRAM PLAN

I. INTRODUCTION

The SCCCMHA Corporate Compliance Program Plan details the specific compliance principles, components, and activities of SCCCMHA as a healthcare provider. SCCCMHA promotes high quality services, tailored to the needs of the individual, provided by persons with a duty of care who adhere to the highest ethical standards. SCCCMHA wishes to deter fraudulent activities, detect misconduct and prevent waste and abuse of government resources. The overall purpose of the Compliance Program is to act as an internal control.

Efforts to uncover fraudulent practices in the healthcare industry and to encourage public reporting of them were mandated in the 1996 Health Insurance Portability and Accountability Act (HIPAA). Following findings of fraud in several locations by the Office of the Inspector General (OIG), the components of a Corporate Compliance Program acceptable to the Federal government were articulated in several OIG Advisories. In 2006 the Deficit Reduction Act made way for the creation of the Medicaid Integrity Program (MIP). Together, along with the Code of Federal Regulations (CFRs), they call for a standard approach to Medicaid compliance and integrity.

Corporate Compliance Plans are required for providers receiving more than five (5) million dollars in Medicaid funds. Program basics include:

- Designation of a Compliance Officer and Compliance Committee;
- Written compliance standards, policies and procedures; well-publicized disciplinary standards for failure to comply
- Conducting effective training and education for the compliance officer, senior management and employees/contractors;
- Developing and maintaining effective lines of communication;
- Responding timely to detected offenses, implementing corrective action, and issuing discipline / fines as appropriate;
- Conducting internal monitoring and auditing;
- Staying current with the law / regulations; and
- Dissemination of the contact information for reporting fraud, waste and abuse to SCCCMHA, Region 10 PIHP and the MDHHS OIG

The SCCCMHA Corporate Compliance Program receives oversight from the Region 10 Prepaid Inpatient Health Plan (PIHP) Corporate Compliance Office and is contractually required to provide regular reports on its compliance activities to the PIHP.

II. CORPORATE COMPLIANCE OFFICE AND COMMITTEE

SCCCMHA maintains a Corporate Compliance Committee to oversee the Compliance Program. Members include the Associate Director of Administration/Corporate Compliance Officer (Privacy Officer), Information Technology Director (Security Officer) and Administrative Specialist (representing network management). The Committee is charged with developing and recommending an Annual Compliance Plan, including specific outcome goals and compliance improvement/assessment activities. The Annual Compliance Plan is reviewed and approved by the Board of Directors.

Compliance Officer functions have been assigned to the Associate Director of Administration who meets with the Quality Improvement Committee (QIC) and/or Board of Directors on a periodic basis to review compliance issues, advise regarding program policy, policy development, training, and other relevant issues. The SCCCMHA Corporate Compliance Officer reports to the SCCCMHA Executive Director and the Board of Directors.

III. FOUNDATION AND LEGAL BASIS OF PROGRAM

The Corporate Compliance Program is founded on a) the ethical principles that form the basis of the Authority's culture, b) a body of laws which defines actions that constitute criminal behavior and establish civil and criminal penalties, and c) on regulations which implement Federal and State law and prescribe financial sanctions, and/or civil and criminal penalties for violation.

A. Ethical Foundation and Principles:

The Authority subscribes to a unified Code of Ethics which was originally adopted in 1996 and is reaffirmed annually by the Board. Compliance with this ethical foundation is reinforced through the staff evaluation process. Compliance with the ethical foundation by staff in contracted entities is monitored through the Contract Monitoring process.

B. Legal Foundation:

The legal basis of the Compliance Program centers around several Federal and State statutes. It is the overall role of the laws to prevent and detect fraud, abuse and waste.

- The Federal False Claims Act (1863): This Act permits individuals to bring action against parties which have defrauded the government and provides for an award of ½ the amount recovered. The Act contains protection from recrimination against those who report, testify or assist in investigation of alleged violations (whistleblowers) and provides a broad definition of "knowingly" billing Medicaid or Medicare for services which were not provided, not provided according to requirements for receiving payment or were unnecessary. The most common criminal provisions invoked in health care prosecutions are prohibitions against:
    - False claims
    - False statements
    - Mail fraud and wire fraud

  Penalties are:
    - 5 years imprisonment

- Fine of $250K for an individual or $500K for an organization, or 2 times the gross gain or loss from the offense, whichever is greater.
- Mandatory exclusion from participation in federal health care program

- The Michigan Medicaid False Claims Act (1977): An act to prohibit fraud in the obtaining of benefits or payments in connection with the medical assistance program; to prohibit kickbacks or bribes in connection with the program; to prohibit conspiracies in obtaining benefits or payments; to authorize the attorney general to investigate alleged violations of this act; to provide for civil actions to recover money received by reason of fraudulent conduct; to prohibit retaliation (whistleblower's); to provide for certain civil fines; and to prescribe remedies and penalties.

- The Anti-Kickback Statute: Prohibits the offer, solicitation, payment or receipt of remuneration , in cash or in kind, in return for or to induce a referral for any service paid for or supported by the federal government or for any good or service paid for in connection with an individual's service delivery. There is a penalty for knowingly and willfully offering, paying, soliciting or receiving kickbacks; violations are felonies; and maximum fine of $25K, imprisonment of up to 5 years.

- HIPAA (1996): Expands the definition of "knowing and willful conduct" to include instances of "deliberate ignorance" such as failure to understand and correctly apply billing codes. The most severe HIPAA violations call for a prison sentence of up to 10 years.

C. Other legal authority:

Regulations which implement Healthcare Law include:

- Affordable Care Act (2010);
- Social Security Act, 1903(m)(95)(i);
- Code of Federal Regulations (CFR) implementing the Balanced Budget Act of 1996 with respect to the Management of Medicaid Managed Care Programs;
- Medicaid Integrity Program developed pursuant to the Deficit Reduction Act of 2006;
- Advisories issued by the HHS Office of the Office of Inspector General (OIG) for the conduct of Fraud and Abuse Compliance Programs;
- Guidelines for Addressing Medicaid Fraud and Abuse in Managed Care**,** issued by the Department of Health and Human Services; and
- Michigan Mental Health Code (1974; 1996) and Mental Health Administrative Rules, as promulgated by the State.

IV. FUNCTIONS

These functions include the fundamental elements that together build an effective Compliance Program. Functions include ongoing activities in the following areas.

1. Assessment of Risk

The Compliance Officer is responsible for ensuring that practices of both direct operated and contracted Medicaid service providers are such so that the risk of fraud, waste and abuse is understood and minimized. Major areas of potential risk include the following:

- *Network Management/contracting issues*. This may include the potential that subcontractors have inadequate or falsified provider credentials, have falsified

solvency requirements, engage in bid-rigging or collusion among providers or violate standards related to conflict of interest or principal-agent requirements. SCCCMHA is also at risk of having a service array which has inadequate capacity to provide the scope, intensity and duration of services required by Medicaid regulations, or of paying for services at rates which have inadequate economic justification.

- *Inappropriate Utilization issues.* When practices result in a pattern of denying eligible persons necessary services on a timely basis or providing services that cannot be supported by medical necessity criteria, these practices may be considered Medicaid fraud. Other examples include delay in providing services, defining "appropriate care" in a manner not consistent with standards of care, inhibiting the appeal process, an ineffective grievance process, unreasonable prior authorization standards, provider incentives to limit care and routine denial of claims.
- *Claims Submission and Billing Procedures.* Examples include upcoding or inflating claims, double-billing, billing for ineligible individuals or for services not rendered, billing for unnecessary services, or inadequate documentation of services provided.
- *Failure to meet other requirements* of Federal or State law and regulations, including the Balanced Budget Act and HIPAA.

Although embezzlement and theft are clear violations of law, they are generally not within the scope of activity of the Compliance Program, unless one of the risk areas defined above is the mechanism for carrying out the embezzlement/theft.

SCCCMHA, in accordance with "Security Standards for the Protection of Electronic Protected Health Information," found at 45 CFR Part 160 and Part 164, Subparts A and C completes a HIPAA Risk Assessment/Analysis.

The HIPAA Security Risk Assessment, which incorporates Meaningful Use (MU), is completed annually, generally in December. Following the Risk Assessment, a Risk Management Plan is developed to assist in management of identified risk area. Goals and recommendations based on the findings are followed up by the Privacy & Security Committee with on-going reports of progress provided to the Quality Improvement Committee.

2. Policy and Procedure Development, Review and Revision:

The Compliance Officer, with the input of the QIC, Region 10 PIHP, and other resources, will determine what policies if any need to be developed to augment practices already in place to help ensure legal compliance.

Current policies include:

- Conflict of Interest (01-001-0030)
- Corporate Compliance Complaint, Investigation, and Reporting Process (01-002-0020)
- Grievance Process (02-001-0040)
- Appeal Process & Second Opinion (02-001-0045)
- St. Clair Utilization Management (02-003-0011)
- Claims Verification (02-003-0020)
- Protected Health Information – Privacy Measures (08-002-0005)
- Health Care Information Privacy & Security Measures (HIPAA) (08-002-0006)
- OASIS Electronic Health Record (08-003-0005)

3. Prevention Activities/Training:

   The Compliance Officer ensures initial orientation and ongoing training are conducted.

   - All employees, direct and contractual, are trained initially and annually; each new employee of the region is provided with written information and discussion on an individual basis as part of the new employee orientation. Training materials include the compliance training information received from Region 10 PIHP. In addition to training in Corporate Compliance, HIPAA and Confidentiality (Recipient Rights) staff are asked to sign a separate attestation that they understand these training concepts, laws and regulations, including the limitations of the scope of their specific job tasks and "need to know." This attestation reinforces for staff the importance of adhering to these concepts and provides another opportunity for questions.
   - Contract provider entities are responsible for training their staff; or may request SCCCMHA to provide this training on its behalf. Reporting of the training is included in quarterly performance indicators. Documentation of this training is to be kept with personnel files and forwarded as requested.
   - Periodic Corporate Compliance communications are issued to both the direct employees and contract agency system as compliance reminders or when a specific system issue may arise.

4. Ensuring that Information regarding Current Law and Regulation is Disseminated

   The Compliance Officer is responsible for reviewing all new compliance related law, regulation and official interpretation of law, and regulation which is issued by State and Federal agencies for the network. Administrative memos (including e-mails) to employees and/or Policy Alerts will be issued as appropriate.

5. Detection Activities

   The system for detecting noncompliance has two (2) components:
   - The first is a body of auditing and review mechanisms conducted by SCCCMHA staff. These auditing reviews include: Contract Monitoring reviews; Medicaid Claims Verification reviews and Utilization Management reviews. All audit functions are part of the overall Corporate Compliance Program. Reviewers will report the presence of issues that require investigation from a compliance perspective.
   - The second component is a mechanism for confidential reporting of suspected incidents of noncompliant behavior. Staff are also assured that allegations will be held in confidence, to the limit allowed by law, that they will not be penalized for reporting suspected incidents and that fair and objective investigation of all allegations will be conducted prior to any action.

6. Investigation, Disciplinary Activity, Disclosure Activities

   SCCCMHA undertakes investigative activities when a preliminary review of audit and monitoring data or a report of suspected noncompliance indicates reasonable cause to suspect noncompliance is occurring. Documentation of all investigations and outcomes is maintained. SCCCMHA reports to the Region10 PIHP and/or MDHHS as required.

7. Assessment and Evaluation of Compliance Program

The annual assessment of the Compliance Program will determine whether the required elements have been implemented and whether activities have resulted in meeting the established goals. Key indicators:

- Analysis of reports generated as part of the Medicaid Claims Verification reviews and Utilization Reviews to identify potentially abusive claims payment and service provision practices;
- Analysis of grievance and appeal activities;
- Analysis of complaints related to over or under utilization, denial of access or denial of choice;
- Analysis of all allegations of abuse, waste, and/or fraud;
- Analysis of all complaints relating to HIPAA violations;
- A review and analysis of Compliance activities and provider agencies via the annual contract monitoring process.

The Corporate Compliance Committee shall develop an annual Corporate Compliance Report covering the fiscal year that is ending and an annual Corporate Compliance Plan for the coming fiscal year. These documents are reviewed by the Board of Directors.

Attachment:

A. St. Clair County CMH Authority Corporate Compliance Committee FY 2019 Goals

\\fileshare1\Corporate Compliance\Reports\FY19\CORP COMPLIANCE PLAN FY2019.doc

St. Clair County CMH Authority

QUALITY IMPROVEMENT PLAN: FY 2019

-- Corporate Compliance Annual Goals --

PRIORITY GOALS/KEY TASKS	ACCOMPLISHMENTS
1. Report monthly on corporate compliance complaints; identify trends (St. Clair CMH). *(Medicaid Integrity Program, Corporate Compliance Plan)*	
2. Report quarterly on Program Integrity activities (i.e., tips/grievances received; data mining, claims analysis; audits; overpayments collected; identification and investigation of fraud, waste, abuse, etc.) *(Corporate Compliance Plan)*	
3. Report monthly on grievance and appeals activities *(Corporate Compliance Plan).*	
4. SCCCMHA Corporate Compliance Committee to meet quarterly or more frequently as deemed necessary.	
5. Monitor and report any legal/regulatory changes. *(Good administrative practice)*	
6. Monitor and report on debarred providers. *(CFR requirement 438.610)*	
7. Provide training and education on corporate compliance *(CFR requirement 438.608)*	
8. Monitor subnetwork providers' corporate compliance activities *(Corporate Compliance Plan)*	
9. Conduct an annual evaluation of the Compliance Plan & report to the St. Clair CMH Board. *(Corporate Compliance Plan)*	

Note: Claims verification and under/over utilization reported under Utilization Management, although part of Compliance Plan.