St. Clair County
Community Mental Health Authority

FY2017

Corporate Compliance Program Plan

CORPORATE COMPLIANCE PROGRAM PLAN

I. INTRODUCTION

The Region 10 Prepaid Inpatient Health Plan (PIHP) maintains oversight of the Corporate Compliance Program for Genesee Health System, Lapeer County Community Mental Health (CMH), Sanilac County Community Mental Health (CMH) Authority and St. Clair County Community Mental Health Authority (SCCCMHA).

The Federal Medicaid Integrity Program (MIP) requires entities receiving more than five (5) million dollars in Medicaid funds to have a Corporate Compliance Plan. SCCCMHA falls under this MIP requirement. This document describes SCCCMHA's Corporate Compliance Program. The entities involved within the thumb region under this Program include Lapeer County CMH and Sanilac County CMH Authority along with St. Clair County CMH.

The Compliance Program covers the specific compliance principles, components, and activities SCCCMHA performs as a healthcare provider. The purpose of the Compliance Program is to provide quality care for all of the individuals it serves by acting as an internal control. SCCCMHA wants to deter fraudulent acts, detect misconduct and prevent waste and abuse of government resources. 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 MIP. Together they call for a standard approach to Medicaid compliance and integrity.

Compliance Plan Program basics include:

- Designating a Compliance Officer and Compliance Committee;
- Written standards, policies and procedures;
- Implement compliance and practice standards;
- Code of conduct;
- Conducting effective training and education;
- Developing effective lines of communication;
- Responding to detected offenses, implementing corrective action, and issuing discipline / fines as appropriate;
- Conducting monitoring and auditing; and
- Staying current with the law / regulations.

II. FOUNDATION AND LEGAL BASIS OF PROGRAM

The Corporate Compliance Program is founded on a) the ethical principles that are the basis of the "corporate" culture of the Authority, 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. Compliance with this ethical foundation is reinforced through the annual 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 four (4) Federal statutes and one (1) State statute. 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. HIPAA calls for a prison sentence of up to 10 years.

C. Other legal authority:

Regulations which implement Federal Healthcare Law contained in the Social Security Act, as amended, include:

- 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.

III. COMPLIANCE PROGRAM PURPOSE

In providing quality care by acting as an internal control mechanism, the elements of the Corporate Compliance Program purpose include:

1. To prevent noncompliance (through education and detection) with applicable law, whether accidental or intentional;
2. To detect noncompliance which may occur;
3. To discipline individuals involved in non-compliance;
4. To prevent reoccurrence of noncompliance.

IV. SCOPE OF PROGRAM AND DELEGATION OF FUNCTIONAL RESPONSIBILITY

SCCCMHA maintains a Corporate Compliance Committee that reports regularly to the Authority's Quality Improvement Council (QIC) and the SCCCMHA Board of Directors. The Compliance Committee consists of staff members who are representative of major departments within SCCCMHA such as quality assurance, information technology and network management. Compliance Officer functions have been assigned to a staff member. The Corporate Compliance Officer meets with the QIC and/or Board of Directors on a periodic basis to review and resolve compliance issues and advise regarding program policy, policy development, training, and other issues.

The Committee is charged with developing and recommending an Annual Compliance Plan, including specific outcome goals and compliance improvement/assessment activities to be undertaken. The Annual Compliance Plan is ultimately finalized and approved by the Board of Directors.

V. FUNCTIONS

The functions of the Compliance Program operationalize the fundamental elements of an effective Compliance Program. This includes ongoing activities in the following areas.

1. Assessment of Risk

The Compliance Officer is responsible for ensuring that practices within operation of its program and its contracted Medicaid service providers are such so that the risk of fraud and abuse is understood and minimized. This function involves assessment of both

existing and planned activity to identify potential risks and the level of that risk. Many areas of risk begin as failures to adequately perform under existing contracts, or policies and procedures; however, if not stopped or when combined with other undesirable practices, they may be considered fraud. Major areas of potential risk include the following:

- Network Management/contracting issues, including 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, it may be considered Medicaid fraud. Examples include delay in providing services, defining 'appropriate care' in a manner not consistent with standards of care, inappropriate Utilization Review Guidelines, inhibiting the appeal process for beneficiaries, 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, and billing for unnecessary services.
- 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 must complete a HIPAA Risk Assessment/Analysis.

The annual HIPAA Security Risk Assessment, which incorporates Meaningful Use (MU), is completed annually. It was most recently completed in December, 2015 and a related Risk Management Plan was developed for 2016. Subsequently, the assessment and plan detail were provided to Management Planning Team in February of 2016 and to the SCCCMHA Board of Directors in April of 2016. Goals and recommendations based on the findings were followed up by the Privacy & Security Committee with on-going reports of progress provided to The Quality Improvement Committee.

2. <u>Policy and Procedure Development, Review and Revision:</u>

The Compliance Officer, with the input of the QIC 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:

- Protected Health Information – Privacy Measures (08-002-0005)
- Health Care Information Privacy & Security Measures (HIPAA) (08-002-0006)

- Corporate Compliance Complaint, Investigation, and Reporting Process (01-002-0020)
- Second Opinion Process (02-001-0035)
- Grievance Process (02-001-0040)
- Appeal Process (02-001-0045)

3. Prevention Activities/Training:

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

   - All employees, direct and contractual, are to be trained; each new employee of the region is provided with written information and discussion on an individual basis as part of the new employee orientation.
   - Contract provider entities are responsible for training their staff; or may request SCCCMHA to provide this training on its behalf. Documentation of this training is to be kept with personnel files and forwarded as requested.

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. Compliance relevant alerts may also be issued when particular compliance problems are suspected.

5. Detection Activities

   The system for detecting noncompliance has two (2) components:
   - The first is a body of auditing and review mechanisms conducted by staff of the provider network. These auditing reviews include: Contract Monitoring reviews; Medicaid Claims Verification reviews, Concurrent Utilization Management reviews, and Retrospective Utilization Reviews. All sub-audit functions are part of the overall Corporate Compliance Program. The function of the Corporate Compliance Program in this regard is to ensure that audits include issues of regulatory concern and that monitoring tools are regularly updated to reflect both existing and new issues. Reviewers will report for 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. In this regard all staff must know that failure to report suspected fraudulent behavior is unethical and thus itself is noncompliant. 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.

7. Assessment and Evaluation of Compliance Program

   The annual assessment and evaluation of the Compliance Program will determine whether the required elements have been implemented as well as whether activities have resulted in

meeting the goals established. Methods that can be used to assess and evaluate the Compliance Program include the following:

- An analysis of reports generated as part of the Medicaid Claims Verification reviews and Utilization Review processes to identify potentially abusive claims payment and service provision practices;
- An analysis of all individuals' complaints to identify potential areas of abuse related to over or under utilization, denial of access or denial of choice;
- An analysis of all allegations of abuse and/or fraud;
- A review and analysis of Compliance activities and provider agencies via the annual contract monitoring process.

The Compliance Officer shall take lead to develop an annual Corporate Compliance Report of this assessment and evaluation and to provide such to key stakeholders. The Compliance Officer takes the lead to update the annual Corporate Compliance Plan if needed.

Where determined necessary, by the Board of Directors, the Authority will ask for an independent review of the Compliance Plan outcomes.

Attachment:

A. St. Clair County CMH Authority Corporate Compliance Committee FY 2017 Goals

St. Clair County CMH Authority
QUALITY IMPROVEMENT PLAN: FY 2017

-- Corporate Compliance Annual Goals --

PRIORITY GOALS/KEY TASKS	ACCOMPLISHMEN
1. Report monthly on corporate compliance complaints; identify trends (St. Clair CMH). *(Medicaid Integrity Program, Corporate Compliance Plan)*	
2. Monitor and report any legal/regulatory changes. *(Good administrative practice)*	
3. Monitor and report on debarred providers. *(CFR requirement 438.610)*	
4. Provide training and education on corporate compliance *(CFR requirement 438.608)*	
5. Monitor subnetwork providers' corporate compliance activities *(Corporate Compliance Plan)*	
6. Conduct an annual evaluation of the Compliance Plan & report to the St. Clair CMH Board. *(Corporate Compliance Plan)*	
7. Report on any other significant events. *(Good administrative practice*	

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