

COMMUNITY MENTAL HEALTH PARTNERSHIP OF SOUTHEASTERN MICHIGAN		<i>Policy and Procedure</i>	
Department Compliance		# of Pages: 6	
Policy Name CORPORATE COMPLIANCE		Type of Policy: <input type="checkbox"/> WCHO <input checked="" type="checkbox"/> Regional <input type="checkbox"/> Network	
Policy Number 01.002	Effective Date	Revision Date	Approval Date 2/8/06
Administrative/Board of Directors Sign Off			
Administrative Signature:			Date:
Board of Directors Signature:			Date:

A. PURPOSE

To establish a policy and procedures that ensures that the Community Mental Health Partnership of Southeast Michigan (CMHPSM) complies with all federal, state, and local laws, rules, and regulations and other standards set forth by accrediting organizations and professional licensure requirements.

B. APPLICATION

All CMHPSM officials, employees, board members, students, volunteers, and providers under contract with the CMHPSM network shall be responsible for abiding by all compliance, confidentiality, and ethics standards as set forth in this policy. Due to the collaborative nature amongst the CMHPSM members, including integrated elements of the data systems, all members of the affiliation (the PIHP and the CSSNs) shall coordinate efforts to ensure the security and privacy of protected health information, and to ensure compliance with all other applicable regulations, laws and standards. External application of standards shall be defined in Chain of Trust Agreements and/or contract language.

C. DEFINITIONS

Risk Assessment or Risk Analysis: The process of selecting appropriate measures to protect against particular dangers to computer systems, data and clinical records.

Protected Health Information (a.k.a. confidential information) - All personally identifiable information and material about a recipient in any form or medium, and the information that an individual is or is not receiving services.

Healthcare Information: Any information, whether oral or recorded in any form or medium that: (a) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and that (b) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual.

D. POLICY

- A. All staff, board members, students, volunteers, and providers with the CMHPSM network shall comply with all federal, state, and local laws, rules, and regulations applicable to the Organization's business lines, as well as other standards set forth by accrediting organizations and professional licensure requirements.
- B. CMHPSM shall ensure the security, privacy, integrity, and confidentiality of all consumer related information in accordance with professional ethics and legal requirements.
- C. Policies and procedures necessary to ensure compliance with federal, state, and local laws, rules, and regulations are set forth in policy and procedure manuals maintained by the members of the Community Mental Health Partnership of Southeast Michigan, and in the Provider Manual issued to providers within the CMHPSM network.
- D. No director or board member of the CMHPSM, or any person with an employment, consulting, or other arrangement with the CMHPSM, can be a person who is debarred, suspended, or otherwise excluded from participating in procurement activities under the Federal Acquisition Regulation, or from participating in non-procurement activities under regulations issued under Executive Order No. 12549 or under guidelines implementing Executive Order No. 12549, or anyone who is an affiliate, as defined in the Federal Acquisition Regulation, of such a person.
- E. Each affiliate has an Ethics policy that has been disseminated to each local network that sets forth specific expectations regarding conduct in the workplace. All CMHPSM staff, board members, students, volunteers, and providers are expected to conduct themselves in an ethical manner while performing their duties.
- F. Sanctions will be enacted against any employee, board member, student, or volunteer of the CMHPSM or its providers who willfully violates this compliance policy. Sanctions are set forth in the CMHPSM Sanctions for Breaches of Corporate Compliance or Confidentiality policy.
- G. To ensure compliance, the CMHPSM shall have an individual identified as the CMHPSM's Compliance Officer. The CMHPSM shall also maintain a Regional

Corporate Compliance Committee charged with the development, coordination, and oversight of the CMHPSM's compliance efforts, including:

- Review annual regional compliance audits to ensure adherence with established policies, procedures, and laws. If deficiencies are detected, require submission of corrective action plans and monitoring of said plans.
- Conduct an annual assessment of the CMHPSM's policies, procedures, and processes to ensure compliance with laws, rules, and regulations. This assessment will focus strictly on compliance with all laws, rules, regulations, and standards, and will not supplant other assigned responsibility for specific policies.
- Review any changes in law, regulations, or standards and identify any areas of need in organizational policy, procedure, and practice.
- Ensure all employees staff, board members, volunteers, and students are trained on relevant laws, rules, and regulations.
- Perform risk analysis and risk management functions necessary to assure the privacy and security of protected health information
- Perform risk analysis and risk management functions necessary to ensure areas of risk are assessed and corrected in compliance with laws, rules, and regulations.
- Monitor regional plans of correction and make any necessary recommendations, including performance improvement activities/recommendations as a result of assessed areas of need.

The Regional Corporate Compliance Committee is also given authority to assign ad hoc members or use specialized consultants to complete its work.

- H. The responsibility for ensuring compliance with the security of health related information shall be assigned to the Regional Corporate Compliance Committee with membership appointed by the Affiliation Executive Committee. The director of each local affiliate shall appoint a local Security Officer to provide local oversight in ensuring local compliance and information dissemination. Each affiliate member of the CMHPSM may also establish a local Compliance/Security committee at their discretion in ensuring local compliance with all laws, rules, regulations, and standards.
- I. Reports of the results of all annual compliance audits shall be shared with the Regional Performance Improvement Committee and the CMHPSM Affiliation Executive Committee.

E. EXHIBITS

None

VI. REFERENCES

- A. Thornton, Mary, Ahead of the Game: A Guide for Corporate Compliance
- B. Regulatory Compliance Notebook of all Applicable Federal and State Laws
- C. 45 CFR, Parts 400 and 438 (Balanced Budget Act)
- D. 45CFR Part 164 (Health Information Portability and Accountability Act)
- E. JCAHO Standards for Behavioral Healthcare Organizations (MCO and HCN)
- F. MDCH PIHP Medicaid Contract
- G. MDCH CMHA Medicaid Contract
- H. MDCH PIHP GF Contract
- I. MDCH CMHA GF Contract
- J. WCHO Policy and Procedure Manual
- K. WCHO Ethics Policy
- L. WCHO Sanctions for Breaches of Corporate Compliance or Confidentiality
- M. CMHPSM Policy on Confidentiality and Access to Clinical Records

VII. PROCEDURES

<u>WHO</u>	<u>DOES WHAT</u>
Affiliate Executive Committee	1. Appoints Regional Compliance Officer
CSSN Executive Director Or Chief Executive Officer	<ul style="list-style-type: none"> 1. Appoints local Compliance Officer. 2. Appoints local Security Officer 3. Provides regular supervision for the Compliance and Security Officer(s) 4. Appoints members to the Compliance Committee
Regional Compliance Officer	<ul style="list-style-type: none"> 1. Scans the federal register and other appropriate websites for promulgation of laws, rules, or regulations related to services provided by the CMHPSM 2. Maintains a library of all pertinent laws, rules, and regulations governing the CMHPSM. 3. Conducts an annual internal audit of the WCHO's Comprehensive Specialty Services Network Providers (CSSN's), using an established assessment instrument, to ensure compliance with laws, rules, or regulations. 4. Assumes responsibilities as the Chairperson of the Regional Compliance Committee, including representing the RCC as a standing member of the Regional Performance Improvement Committee.. 5. Provides training and consultation to all CMHPSM staff and network providers regarding laws, rules, and regulations that pertain to the CMHPSM. 6. Reports quarterly to the Regional Performance Improvement Committee on activities of the Regional Compliance Committee including trends, compliance issues, and

performance improvement activities/recommendations as a result of assessed areas of need.

7. Reports to the Affiliation Executive Committee on compliance activities, regional plans of correction, and areas of need on an as needed basis.

Regional Compliance
Committee/Committee
Members

1. Meets regularly to complete routine business
2. Scheduled additional meetings as needed to address specific areas of need.
3. Reviews all new laws, rules, or regulations to determine
4. implications for the CMHPSM.
5. Recommends changes to policies, procedures, or structure to comply with evolving laws, rules, and regulations.
6. Reviews all regional compliance audits, making suggestions for improvement and/or requesting corrective action plans as appropriate.
7. Assigns charges relevant to areas of need in assuring compliance to the appropriate committee, group, or individual as needed.
8. Conducts (at minimum) local semi-annual security/privacy risk assessments and reports these results to the committee.
9. Conducts an overall local compliance risk assessment and risk analysis every three years and reports these results to the committee.
10. Risk assessment and risk analysis will include:
 - Identification of assets.
 - Assessment of potential risks, vulnerabilities, and current controls, including threats to confidentiality, integrity, and availability of information.
 - Development of plans to address identified risk
 - Recommendations regarding expenditures to address identified needs, selecting cost effective control measures which balance the costs of proposed measures with the human and financial risks of potential loss and harm.

The risk assessment shall be updated whenever there is a significant change in circumstances, laws, rules, regulations or standards.

11. Reviews implementation plans for introduction of new data systems/elements with compliance implications.
12. Reviews regional audits and plans of correction to assure compliance and review any areas of need.
13. Reviews data related to any breaches of related confidentiality policies and standards to determine appropriate systems corrections and to assure that sanctions

were applied appropriately.

- | | |
|-----------------------|---|
| Regional PI Committee | <ol style="list-style-type: none">14. Reports on a quarterly basis to the Regional PI Committee on audits, plans of correction, compliance issues, confidentiality breaches and performance improvement activities/recommendations as a result of assessed areas of need.1. Reviews the summary reports of the Compliance Officer and Regional Compliance Committee, including local and regional outcomes.2. Makes recommendations for enhancing or improving the compliance process as necessary. |
|-----------------------|---|