	General Policy			
	Chapter:	HIPAA	Policy #	7-1-1
	Section:	HIPAA Privacy and Security	Revision #	5

- I. **PURPOSE:** To provide for plans and procedures to comply with the HIPAA Privacy Rule to protect the privacy and security of personal health information; and the HIPAA Security Rule to ensure the appropriate administrative, physical, and technical safeguards of the system components that such data resides in.
- II. **APPLICATION:** All personnel of WMCMH.
- III. **REQUIRED BY:** The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Department of Health and Human Services privacy and security regulations implementing HIPAA, HITECH Act of 2009, other federal and state laws protecting confidentiality of personal health information, professional ethics, and accreditation requirements.

IV. **DEFINITIONS:**

DHHS – Department of Health and Human Services

HIPAA – Health Insurance Portability and Accountability Act of 1996

Privacy Officer—The WMCMH Privacy Officer is the Director, Corporate Compliance and Risk Management


Security Officer – The WMCMH Security Officer is the Director, Information Services

- V. **POLICY:** It is the policy of West Michigan Community Mental Health to provide for the protection of individually identifiable health information. West Michigan CMH has implemented and revised policies, procedures and plans to safeguard individually identifiable health information. The referenced policies and procedures detail these mechanisms.

If any standards specified in the referenced policies and/or procedures are violated, immediate sanctions will occur accordingly

VI. **PROCEDURES:**

1. The HIPAA Security Rule Policy is a result of a thorough Risk Analysis (copy of Risk Analysis will be held by the Security Officer). A Risk Analysis will be conducted as new assets are acquired that may pose additional risk.
2. The Corporate Compliance Committee will review any Risk Analysis completed on new assets, to ensure HIPAA Security Rule compliance.
3. Specific procedures addressing all necessary elements of the HIPAA Privacy and Security Rule are listed below:

	General Policy			
	Chapter:	HIPAA	Policy #	7-1-1
	Section:	HIPAA Privacy and Security	Revision #	5

Code of Ethics

See:

- Policy 4-2-1 (Code of Ethics)

Access Authorization, Access Establishment, and Access Modification

Procedure See:

- Policy 2-2-1 (Care Planning, Documentation, and Coordination)
- Policy 5-2-1-1 (Security of Protected Health Information (PHI) and Safeguarding Customer Clinical Records)

Training Procedure

See Below:

- Policy 4-6-2 (Orientation to Employment)
- Policy 4-6-4 (Training and Development)
-

Report Procedure

See:

- Policy 6-1-3 (Open Lines of Communication)
- Policy 6-1-7 (Compliance Enforcement and Discipline)

Response Procedure

See:

- Policy 6-1-3 (Open Lines of Communication)
- Policy 6-1-4 (Handling Allegations of Non-Compliance)
- Policy 6-1-7 (Compliance Enforcement and Discipline)
- Policy 7-1-2 (Breach Notification)

Data Backup Procedure

See:

- Policy 3-8-2 (Network Backup)

Emergency Management Guide

Internal Audit Procedure

See:

- Policy 2-2-1 (Care Planning, Documentation, and Coordination)
- Policy 2-2-2 (Clinical Records Elements and Organization)
- Policy 2-2-5 (Security of Electronically Stored Clinical Information)
- Policy 3-8-4 (Protection from Unauthorized External Access)
- Policy 3-8-5 (Protection from Unauthorized Internal Access)
- Policy 5-2-1-1 (Security of Protected Health Information (PHI) and Safeguarding Customer Clinical Records)
- Policy 5-2-1-2 (Release of Information)

Combined Security and Privacy Business Associate Agreement


See:

- Policy 6-1-8 (Business Associate Agreement)

Emergency Access Procedure

See:

- Policy 2-2-1 (Care Planning, Documentation, and Coordination)
- Policy 5-2-1-1 (Security of Protected Health Information and Safeguarding Customer Clinical Records)

	General Policy			
	Chapter:	HIPAA	Policy #	7-1-1
	Section:	HIPAA Privacy and Security	Revision #	5

E-mail Procedure

See:

- Policy 3-8-3 (Electronic Communications)

Personnel Security Procedure

See also:

- Policy 4-4-1 (Employee Personnel File– General Policy)
- Policy 4-6-1 (Background Checks)
- Policy 4-6-2 (Orientation to Employment)
- Policy 4-6-3 (Performance and Competency Assessment)
- Policy 4-6-4 (Training and Development)

Videoconferencing Procedure

- Policy 2-2-1 (Care Planning, Documentation, and Coordination)
- Policy 3-8-3 (Electronic Communications)

Cell Phone Procedure

See:

- Policy 3-8-3 (Electronic Communications)

Access Establishment Modification Procedure

- Policy 5-2-1-1 (Security of Protected Health Information and Safeguarding Customer Clinical Records)

VII. SUPPORTING DOCUMENTS: See above.

VIII. POLICY/PROCEDURE REVIEW:

REV#	APPROVED BY	Policy/Procedure	DATE
1	Unknown	Procedure	8/07
2	TinaB	Procedure	1/15
NC	TinaB		2/16
NC	TinaB		5/17
NC	KarenH		5/19
3	Kevin Wilske	Procedure	8/21
4	Corp Comp Comm	Procedure	7/22
4	Corp Comp Comm	Annual Review	7/23
5	Corp. Comp Comm	Procedure	7/24
Board Approval Date: 4/19/2005			

IX. CHIEF EXECUTIVE OFFICER ENDORSEMENT:

I have reviewed and approve of policy # 7-1-1 Revision # 5.

CEO: Lisa Williams

Approval Signature: _____