Third-Party/External Provider Computer Acceptable Use Agreement

montcalm care network **611 North State Street Stanton MI 48888**

A separate "Third-Party Computer Acceptable Use Agreement" form must be completed, signed, and submitted for each person within your organization who needs to access Montcalm Care Network (MCN) Electronic Medical Record (EMR). Each person will be given a unique user ID with system access based on job responsibilities and their "need to know".

WRITTEN AGREEMENT: I, , will:

- Use MCN's Electronic Medical Record (EMR) system or other assigned computer system on a "need-to-know" basis only;
- Retrieve or enter information about consumers as required for clinical care or business functions related to that clinical care only as it relates to my job duties and licensing;
- Remember that it is my legal obligation to protect the privacy and security of all Protected Health Information (PHI) and will take all reasonable precautions to protect the privacy and security of consumer information. This includes protecting my password and not leaving display screens or printed materials containing Protected Health Information (PHI) where it can be viewed inappropriately;
- Change my password so that it is known only to me and will keep it secure;
- NOT disclose my password or allow another person to log in using my User ID and password
- NOT log on using someone else's User ID and password, I understand doing so is fraud and not allowed in any circumstance

All users of MCN computer systems are bound by this agreement.

Staff e-mail address:		Phone #:	
Provider/Organization Name:		Provider Phone #	
Job Title:		Job Duties:	
Signature Credentials:			

I will notify Montcalm Care Network of any changes in my licensure. I am aware that I need to sign a new Acceptable Use Agreement which states any change in name, licensure & resulting changes in job duties.

Staff Types:			
Staff Signature:		Date:	

As Supervisor of the above-listed employee, my signature below indicates that :

- I have read and understood this document, including sections "A" (HIPAA) and "B" (HITECH) on page 2, and I assure that all stated requirements will be met.
- I agree to contact Montcalm Care Network immediately if the above-listed employee no longer needs access rights to MCN's EMR system so that the appropriate security measures can be taken to discontinue access rights.

Supervisor Name:		Signature Credentials:	
Supervisor Signature:		Date:	
Supervisor e-mail address:			

NOTE: MCN Finance department to retain agreement forms for a minimum of seven (7) years.

This section: For Internal MCN Use Only	
User Log-In / ID:	
Functions Assigned to the above user:	☐ External Progress Notes ☐ AP Claims Data Entry ☐ Provider EDI Submissions ☐ External Provider PCP view ☐ Autism ☐ Residential Note ☐ Autism Module ☐ LOCUS ☐ Incident Report-Add ☐ Incident Report-Add Scan ☐ Incident Report-Supervisor ☐ External ABD/Assess/Ref ☐ Provider IPOS Training
IT or Finance Signature:	Date:

montcalm care network 611 North State Street Stanton MI 48888

Section A:

Relates to the Health Insurance Portability and Accountability Act (HIPAA) of 1996:

The HIPAA Security Rule requires Covered Entities to implement "Unique User Identification" standard for electronic systems with Protected Health Information (ePHI). Unique User identification is a unique name or number used to identify and track specific individuals using ePHI systems, also referred to as "Login ID" or "User ID". This provides a means to verify the identity of the persons using the system. The User ID should only be used by the intended person; use by someone other than the intended person is a violation of the HIPAA Security Rule and is fraud. Licensed health professionals who share their password may also be in civil and criminal violation of licensure law. You must have a separate ID for each provider, and it is your responsibility to ensure you are signed on correctly at each location. In other words, while you are working for Provider X, you must log in using the User ID assigned for Provider X and not another provider.

For additional information, see the HIPAA Security Rule section 45 CFR 164.312 (Technical Safeguards) @ http://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-312.pdf

Section B:

Relates to the Health Information and Technology for Economic and Clinical Health (HITECH) Act:

The HITECH Act imposes data breach* notification requirements for unauthorized uses and disclosures of "unsecured PHI" (Protected Health Information), (or basically unencrypted PHI), and Business Associates are now required to also comply. Business Associates are required to report security breaches to covered entities consistent with the requirements, and are also subject to civil and criminal penalties under HIPAA if certain conditions exist. Civil penalties for willful neglect are increased under HITECH; up to $250,000, with repeat/uncorrected violations extending up to $1.5 million.

The HITECH Act requires that patients be notified of any unsecured breach and their PHI might have been accessed, acquired, or disclosed as a result of that breach. If a breach impacts 500 patients or more, then the Health and Human Services (HHS) must be notified, and also prominent media outlets of the geographic area will need to be notified. A Business Associate of a covered entity shall notify the covered entity of a breach, including identification of each individual who's PHI has been breached. A breach is considered discovered on the first day that any employee, officer, or agent of an entity or associate becomes aware that the breach occurred.

All required notifications must be made within sixty (60) calendar days of the discovery of the breach. Burden of proof of all notifications falls on the entity or Associate. Written notification to individuals (or guardians or next of kin) by first class mail to the last known address is required. If contact information is insufficient or out-of-date, a conspicuous notice can be provided on the entity's web page or a notice can be placed in print or broadcast media including a toll-free number to call for more information. If notification is urgent, a telephone call can also be used in conjunction with other forms of notification. Notice of a breach shall include:

- A brief description including the date of the breach and the date of discovery, if known
- A description of the types of PHI included in the breach
- Steps the individual should take to protect themselves from harm from the breach
- A brief description of how the covered entity is investigating, mitigating, and protecting against future breaches
- A toll-free telephone number, e-mail address, website, or postal address to contact for more information

* the term "breach" means the unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

For additional information, see 45 CFR section 13402 of the HITECH Act for details about breach notification @ http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf