|  |
| --- |
| **MONTCALM CARE NETWORK** **611 North State Street, Stanton, MI 48888**  |
|  SUBJECT: HIPAA Reasonable Safeguards  |  Section: 11850  |
|  Effective Date: January 28, 2003  |  Revised Date: April 23, 2016  |
|  Version: 3  |  Status: Current  |

**Reasonable Safeguards:**

Montcalm Care Network shall make reasonable efforts to prevent uses and disclosures that are not permitted in the Privacy Rule. Montcalm Care Network also has addressed reasonable safeguards in the Montcalm Care Network's Confidentiality (#8906) and Management of Information Systems (11927A). This includes having reasonable administrative, technical and physical safeguards in place to prevent such impermissible uses and disclosures. In determining what safeguards are “reasonable,” Montcalm Care Network will use the viewpoint of a prudent health care professional.

Reasonable safeguards must be taken to prevent disclosure of information beyond that which is minimally necessary and to prevent disclosure of information to persons who do not need the information to perform their job function. (see also #8906A Disclosure of Recipient Records, #8230 Integrity and Security of Client Records, #7135 Code of Ethics, and #7136 Rules of Conduct)

Some of the reasonable safeguards Montcalm Care Network will take, include:

* Employees are responsible for taking reasonable precautions to keep consumer medical records out of view of other consumers and those who do not need access to perform their jobs.
* Employees are responsible for putting away any documents containing protected health information (PHI) at the end of the day.
* Employees are responsible for taking precautions and using judgment when leaving messages on answering machines.
* Montcalm Care Network will only send correspondence with consumer information in envelopes and not on exposed postcards.
* PHI is not to be transmitted electronically via email or the Internet unless such transmission is performed on a Montcalm Care Network approved, secured connection between Montcalm Care Network and an authorized sending/receiving party.
* Employees are not permitted to discuss consumer PHI for inappropriate purposes, or purposes outside of their need to know to conduct MCN business.
* Employees are responsible for properly safeguarding PHI that is contained in files and computers when traveling and when the information is at home.

**Safeguarding Computers:**

In addition to the HIPAA security regulations, the HIPAA privacy regulations require that technical safeguards be put in place to safeguard protected health information (PHI).

If a computer contains (PHI), access to the computer shall be protected by the use of passwords. Each employee is responsible for keeping his or her password confidential. Employees shall not use their name as a password or any other word that could be easily guessed by others. Employees shall not share computer passwords. Employees shall log out of the computer if the computer will be left unattended. Employees will be asked to sign a confidentiality agreement agreeing that they will only access the computer for information that they need to know and will not attempt to access the computer if they are not authorized to do so. (See also #11927A Management of Information Systems and #8906 Confidentiality)

1. Employees shall take reasonable precautions to safeguard information from unintended disclosure.
2. Employees shall take reasonable precautions to safeguard information so that only the minimal amount of information necessary to serve the stated purpose is either used or disclosed.
3. Employees shall take reasonable precautions to safeguard information so that information is not disclosed to people who do not have a need to know the information.
4. All employees will be asked to sign a security/need to know agreement.

AUTHORITIES:

45 CFR 164.530

45 CFR 164.514