MONTMORENCY COUNTY COMMISSION ON AGING **Origination Date: 09/09/11**
MONTMORENCY COUNTY, MICHIGAN **Revision Date(s):**

ORIGINATOR/DEPARTMENT: Executive Director

DISTRIBUTION LIST: M.C.C.O.A. Employees,
Board Members & Volunteers

TITLE: Privacy Policy, MCCOA.p.02

POLICY:

Montmorency County Commission on Aging is committed to safeguarding all information including history, records and discussion regarding MCCOA employees and the individuals they serve. In this effort, MCCOA will abide by all appropriate funding regulations. Individual program guidelines may require additional policy and procedures regarding confidentiality.

DEFINITION:

For purposes of this policy, references made to personally identifiable information, protected personal information, or Protected Health Information (PHI) can be defined as any individually identifiable information collected and maintained in a record by MCCOA. This includes information about an individual's education, demographics, financial transactions, medical information, criminal or employment history, or other assigned identifying symbol.

PROCEDURE:

- Staff will not disclose any personally identifying information, health-related or otherwise, including whether or not the individual is being served or was served by the organization.
- Staff will not discuss any individual record with unauthorized individuals during or after work hours. All staff is required to sign the Confidentiality Acknowledgment stating their responsibility and commitment toward protecting participant, fellow staff and their own privacy.
- All staff is required to adhere to the procedures within this Privacy Policy and Notice of Privacy Practices.

DISCLOSURE CONDITIONS:

Disclosure of information can be done only after the following conditions are met:

- Any disclosures made will include only the minimum information necessary to accomplish the purpose of the disclosure.
- Receipt of a court order that is signed by a Judge. Authorization must be obtained from the Executive Director or Privacy Officer before releasing any information under this condition. Requests or orders for information that are drafted by attorneys, unless accompanied by participant authorization, will not be honored. As a courtesy, should a subpoena be received, the program participant should be notified.
- For each disclosure request, a general Authorization for Release of Information form must be signed and dated by the client or employee, and be on file before any information can be released. When protected personal information (including health information) is involved, and the information being disclosed is for purposes other than treatment, payment, health care operations, or normal program administrative functions, the authorization form must include, at a minimum, the specific elements identified in Attachment A-Authorization for Use or Disclosure of Protected Personal Information.
- For a listing of disclosures requiring or not requiring use of the Authorization for Use or Disclosure of Protected Personal Information form, see the reverse side of Attachment A.

- In case of a bona fide emergency (a case in which the medical information is necessary for the immediate care of the client), the information can be released. Document the entire transaction in the client file. Request the client mail an authorization at a later date.

HANDLING OF INFORMATION:

- Programs that involve Personally Identifiable Health Information (PHI) must ensure that all subcontractors receiving or exposed to PHI, have a Business Associate Agreement (Attachment B) incorporated as a part of its normal contracting process. All other contracts must include language, which addresses confidentiality. See Attachment C for sample language.
- No participant/employee information will be given over the telephone, cellular phone, or facsimile to any **unauthorized** person without a completed Authorization form.
- Individuals are guaranteed specific legal rights regarding their personal information (including health information). These rights include, but are not limited to:
  1. The right of access to inspect and obtain a copy of protected information about the individual contained in a designated record set.
  2. The right to amend protected information.
  3. The right to request an accounting of disclosures.
  4. The right to revoke an authorization for use or disclosure of protected information.

  Other specific privacy rights are referenced in the MCCOA Notice of Privacy Practices.
- All facsimile cover sheets and email messages containing protected information must include a statement regarding confidentiality of the message's content and request to contact sender should the message be received in error. See MCCOA's Technology Policy for message language.
- Disclosure of information can be provided to the individual or their personal representative. Personal representatives are required to produce evidence of their authority to act on the person's behalf. Proof of authority may take one of the following forms: notarized power of attorney for healthcare purposes; a court order of appointment of r purposes of guardianship or conservator; or an individual who is the parent of a minor child.
- Non-custodial parents cannot be denied access to records or information concerning his/her child because the parent is not the child's custodial parent unless the parent is prohibited from having access to the records or information by a protective order. (Michigan Child Custody Act).
- Disclosures for purposes other than treatment, payment, health care operations, or normal administrative functions of a program, must be documented on the Accounting of Disclosures Log (Attachment D).
- Inadvertent or unintentional disclosures must be documented on the Accounting of Disclosures Log (Attachment D) and reported to the Program's Privacy Officer and must include corrective action taken. The NEMCSA Privacy or Security Incident Report Form is to be used for documentation. (Example: Documentation was faxed to the wrong entity; requested receiving entity to destroy document).
- Health-related disclosure authorizations must be retained in the participant file for seven years. Retention policy for general disclosures will otherwise be governed by respective program guidelines.
- Destroying Documents: Any unneeded documents of an official nature or otherwise (i.e. scratch notes, messages, etc.) containing identifying information must be shredded or incinerated. Official program documents will be shredded/incinerated per respective program guidelines and time recommendations.
- Destruction of Documents with Outside Vendors: Documentation of a transfer of custody for purposes of destruction of confidential records with commercial document destruction vendors must be maintained within each department. Documentation must include date of transfer, vendor name and summary of records to be destroyed.

SECURITY OF INFORMATION:

- Any personally identifiable information regarding MCCOA program participants or employees is not to be left unattended in plain view. This includes documents or files on staff desks or computer screens. When leaving a workstation for any length of time, sensitive materials are to be secured, for example, place documents in a desk drawer, log off of computer, close calendar, etc. When information is stored in locked file cabinets, keys are to be stored in a secure, non-public area.
- Any medical information maintained on MCCOA program participants or employees is to be housed in locking file cabinets.
- Transporting personally identifiable client or employee information in vehicles or other means of travel must be accomplished in a secure manner. Precautions include, but are not limited to, carrying the information in a secure tote such as a briefcase; confidential information is not to be left exposed or in plain view; vehicles are to be locked when confidential information is transported and/or left unattended.
- Information maintained in home offices is to be secured at all times in the same manner as described in the previous bullets, i.e. confidential information is not to be left exposed or in plain view; using locking file cabinets when appropriate; protecting computer screen from unauthorized viewing, etc.

NOTICE OF PRIVACY PRACTICES:

The Notice of Privacy Practices will be provided to all MCCOA program participants, volunteers, employees, and other appropriate entities. This Notice is available to all other persons upon request.

When the Notice of Privacy Practices is distributed to an individual, staff must make a good faith effort to obtain a signed Acknowledgment of Receipt (Attachment E). Should an individual refuse to sign an Acknowledgement of Receipt or for some other reason it is not possible to obtain the Acknowledgment, staff must document their effort in the client file and the reason it could not be obtained.

The Privacy Officer will retain a copy of the Notice of Privacy Practices, and any revisions to the Notice, for a period of six (6) years form the date they were last in effect.

The Notice of Privacy Practices incudes prominent and specific language that indicates the importance of the Notice. The Notice describes all uses and disclosures of protected information the agency is permitted or required to make without authorization, including uses for treatment, payment, or health care operations. The Notice includes at least one example of the types of uses and disclosures permissible. All other uses or disclosures of protected information will be made only with the person's authorization. See the reverse side of Attachment A-Authorization or Use or Disclosure of Protected Personal Information for a detailed listing of allowable and unallowable use and disclosure information.

DISTRIBUTION PROCEDURE:

- The Notice of Privacy Practices will be distributed at the time of registration for services, new hire orientation, and prior to obtaining a signature on the Authorization for Use or Disclosure of Protected Personal Information form.
- Copies of the Notice will be available upon request from program staff, the Executive Director and/or Privacy Officer
- Copies of the Notice are to be posted and available in all senior centers and office locations.
- The Notice, or any subsequent revisions, will be prominently available through the agency's website at **www.montmorencycoa.org.**
- When there is a language or reading barrier, alternate arrangements will be attempted to provide the information in the Notice of Privacy Practices to the requester.

- Each program is responsible for developing procedures to obtain an "Acknowledgment of Receipt" when distributing the Notice. The Acknowledgement is to be retained for six (6) years. This can be easily accomplished by incorporating the process as part of the intake procedure for program participants and staff.

ACCESS TO INFORMATION:

An individual has the right of access to inspect and obtain a copy of personal information that is maintained by MCCOA regarding that individual. **All requests for access to information must be in writing.** The Privacy Officer will be responsible for monitoring requests for access by individuals. Inspections and copies are to be provided within 30 days of the request if the information is maintained on site or within 60 days if it is maintained offsite.

Neither an individual nor their authorized representative has the right to access psychotherapy notes, information that is compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding. In addition, an individual may be denied access if the information on file was obtained from an entity other than MCCOA under a promise of confidentiality and the access request would be likely to reveal the source of the information. If an individual is denied access, a written denial is to be provided to the individual explaining the basis for the denial and how the individual may complain to MCCOA or the Secretary of the U.S. Department of Health and Human Services (see Notice of Privacy Practices, "To File a Complaint" section).

One request per 12-month period will be provided at no cost. A cost-based fee for copying, mailing, and other supplies may be charged for additional requested copies.

AMENDMENT OF PROTECTED INFORMATION:

MCCOA shall comply with applicable laws as they pertain to an individual's right to have his/her protected health information which is maintained in a designated record set, or other protected information about the individual, amended. **All requests for amendment of protected information must be in writing.**

The designated record set for which a person may request an amendment include:

- Medical records;
- Billing records; or
- Other records that contain protected information that is used to direct treatment or secure services.

Upon receiving a request for amendment, MCCOA shall act on the request generally within sixty (60) days. A single 30-day extension is allowed if MCCOA is unable to comply with the deadline. The Program Privacy Officer will review the request and make an initial determination as to whether the agency can comply with the request. The basis upon which the Program Privacy Officer will make this determination is as follows:

- If the information or record was not created by MCCOA, the individual must provide a reasonable basis to believe that the originator of the information is no longer available to act on the request. If the individual does not meet this stipulation, the Program Privacy Officer can deny the request.
- If the information requested is not part of the agency's designated record set, the request can be denied.
- If the protected information or record is accurate and complete, the request can be denied. To make this determination, the Program Privacy Officer shall confer with the appropriate parties to review the documented information and the request.

When the agency denies a request for amendment, the Program Privacy Officer shall provide the denial in writing. The written notification must contain the following:

- the basis for denial;
- a statement regarding the individual's right to submit a written statement disagreeing with the denial and the procedure for filing such a statement; and
- a description of how the individual may complain to the agency, pursuant to the agency's complaint process and shall also include contact information for the Secretary of the Department of Health and Human Services, pursuant to HIPAA regulations.

All requests for amendments, denials of the request, statements of disagreements, and agency rebuttals shall become part of the individual's designated record set.

ACCOUNTING OF DISCLOSURES OF PROTECTED INFORMATION:

An individual has a right to receive an accounting of disclosures of protected information held by the agency, or an employee of the agency, during a time period specified up to six (6) YEARS PRIOR TO THE DATE OF THE REQUEST. The following disclosures are exempt from the requirement to provide an accounting:

- to carry out treatment, payment, health care operations, as permitted by the individual's consent, for normal program administrative functions, or as otherwise permitted under law;
- to the individual, or their authorized representative, about his or her own information;
- for the agency directory or to persons involved in the individual's care, or other notification purposes permitted under law;
- for national security or intelligence purposes; or
- to law enforcement officials as permitted under law.

The written account must contain the date of the disclosures, name of the person who received the information, and a brief description of the information disclosed, and the purpose of the disclosure. See sample form-Attachment D.

The individual's request must be acted upon no later than sixty (60) days after receipt. If unable to provide the accounting within this time period, an extension may be allowed for no more than an additional thirty (30) days. A cost-based fee may be charged for more than one request within a twelve month period.

MITIGATION:

MCCOA shall mitigate, to the extent possible, any harmful effect known by us to have resulted from a use or disclosure of protected information in violation of federal and state Privacy laws.

REPORTING BREACHES:

A breach notification must be made using an Incident Report when an individual's first name or first initial in combination with any of the following data elements: social security number, drivers' license or state identification number if data elements are not encrypted. The Incident report will be submitted to the Privacy Officer as soon as the breach has been identified. The Privacy Officer will convene a response team as necessary to assess the likely risk of harm and the level of impact to determine when, what, how and to whom notification should be given outside the agency.

COMPLAINTS:

All complaints regarding protected personal information are to be forwarded to the Program's Privacy Officer. All complaints received, and their disposition, shall be documented in written form. The documentation will be retained for six (6) years. HIPAA requires that individuals be informed that they may also complain directly to the Secretary of the Department of Health and Human Services.

WORKFORCE TRAINING:

MCCOA shall provide training to all employees and volunteers on the policies and procedures with respect to protected personal information, as necessary and appropriate to carry out their functions.

For new hires, the training shall be incorporated as part of the orientation process. Employees whose functions are affected by a material change in policies or procedures, or who change positions within the agency, shall receive additional training within a reasonable period of time after the change becomes effective.

All training shall be documented in written or electronic form and shall be retained for seven (7) years.

SANCTIONS:

MCCOA shall apply appropriate sanctions against members of its workforce who fail to comply with the Privacy Policies and Procedures or HIPAA regulations. All sanctions are to be documented in the Personnel record and will be retained indefinately.

MCCOA shall not apply sanctions in an effort to intimidate or retaliate against its workforce for filing a complaint with the Secretary of the Department of Health and Human Services, participating in an investigation or compliance review, or for other reasons specified within the applicable laws and regulations.

Sanctions may vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of protected information.

Sanctions may range from a verbal warning to a written warning, suspension, or termination. MCCOA may apply stronger sanctions (such as termination) without first using milder sanctions (such as a warning) if the violation is severe in its professional judgment, or if there is a pattern of multiple violations.

SOCIAL SECURITY NUMBERS:

In addition to the preceding privacy policies and procedures, MCCOA employees are prohibited from accessing, viewing, or using other employees' or program participants' social security number and identification information. Any employee or individual that accesses social security data without authorization or for illegal purposes shall be disciplined including discharge, and, if illegal intent is determined, referred to authorities for possible criminal prosecution. All documents containing social security numbers and information will be kept in a secure environment with a need-to-know access by authorized personnel only. Disposal methods will be by approved means described abov3.

Specific prohibited uses of social security numbers include:

1. Public display of all or more than four sequential digits.
2. Use of all or more than four sequential digits as a primary account number.
3. Visibly print all or more than four sequential digits on any identification card.
4. Require an individual to transmit all or more than four sequential numbers over the internet or a computer system unless the connection is secure or the transmission is encrypted.
5. Require an individual or use all or more than four sequential digits to gain access to the internet or a computer system.
6. Include all or more than four sequential digits in any document or information mailed to a person unless certain conditions apply.

Additional information regarding the Social Security Privacy Act 454 of 2004 may be obtained from the MCCOA Privacy Officer.

DATED: _____ _____

Anna M. Rogers, Executive Director