The Commonwealth of Massachusetts
Executive Office of Elder Affairs
One Ashburton Place, Boston, MA 02108

ARGEO PAUL CELLUCCI
GOVERNOR

FRANKLIN P. OLLIVIERRE
SECRETARY

Phone (617) 727-7750
Fax (617) 727-9368

PROGRAM INSTRUCTION

EOEA-PI-97-55
(reference EOEA-PI-97-49)

To: Area Agencies on Aging
Home Care Corporations
Nutrition Projects
Protective Services Agencies
Ombudsman Programs
EOEA Contractors Holding Personal Data
Interested Agencies

From: Franklin P. Ollivierre

Date: December 26, 1997

Subject: Clarification of Client Privacy and Confidentiality Policies Resulting From Consolidation of EOEA Privacy and Confidentiality Regulations

****

As you know, pursuant to Executive Order #384, our Privacy and Confidentiality Regulations (other than those affecting Protective Services Programs) are being consolidated into an Executive Office for Administration and Finance regulation (801 CMR 3.00 et seq.) (See EOEA PI-97-49). Under the statute which governs these regulations, (M.G.L. c. 66A, the Fair Information Practices Act) Executive Office of Elder Affairs (EOEA) and contractors which "hold" personal client data for us in the course of performing their contracts are required to perform several important duties in the collection, use, maintenance or dissemination of personal data, including, but not limited to the following:

1. identify an individual responsible for the contractor's personal data system and educate that person about design, development, operation and maintenance of the personal data system and the rules and remedies available to individuals whose rights are affected by the holding of data;
2. not allow any other agency or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulations which are consistent with the purposes of this chapter;
3. take reasonable precautions to protect personal data from dangers of fire, theft, flood, natural disaster, or other physical threat;

4. inform in writing an individual upon his request whether he is a data subject, and if so, make such data fully available to him, unless doing so is prohibited by law;
5. maintain personal data with accuracy, completeness and relevance and not collect more personal data than are reasonably necessary for the performance of the statutory functions;
6. establish procedures that allow each data subject to contest the accuracy, completeness, pertinence, timeliness, relevance or dissemination of his personal data or denial of access to such data; and
7. maintain procedures to ensure that no personal data are made available in response to a demand for data made by compulsory legal process (e.g. a subpoena) unless the data subject has been notified of such demand in reasonable time to have the process quashed.

As part of this process, we would like to:

1. attach a copy of 801 CMR 3.00, et seq.;
2. clarify certain policies and procedures regarding the privacy and confidentiality of the client case records of EOEA contractors as so called "supplementary privacy and confidentiality policies;" and
3. clarify that any agency, individual or entity which holds personal data under an arrangement, understanding or ongoing contract, or subcontract, grant or agreement with EOEA on December 25, 1997 shall in consideration of receipt of funding and continuation of performance continue to be a Holder of Personal Data under M.G.L. c. 66A, s. 1, et seq., Executive Order 111, 801 CME 3.00, et seq. applicable regulations and section 6 of the Commonwealth Terms and Conditions for Human and Social Services on and after December 26, 1997, during the term of such agreement.

We hope to be able to provide training on issues related to Privacy and Confidentiality in the near future.

If you have any questions, please call Joel M. Semuels, Acting General Counsel at (617)222-7461.

The Commonwealth of Massachusetts
Executive Office of Elder Affairs
One Ashburton Place, Boston, MA 02108

ARGEO PAUL CELLUCCI
GOVERNOR

FRANKLIN P. OLLIVIERRE
SECRETARY

Phone (617) 727-7750
Fax (617) 727-9368

SUPPLEMENTARY PRIVACY AND CONFIDENTIALITY POLICIES OF THE EXECUTIVE OFFICE OF ELDER AFFAIRS (EOEA) FOR EOEA AND HOLDERS OF PERSONAL DATA UNDER AGREEMENT WITH EOEA.

12/26/97

1. Scope and Purpose

This Program Instruction provides supplementary privacy and confidentiality policies to M.G.L. c. 66A, Executive Order 111, 801 CMR 3.00 et seq. and where applicable, 651 CMR 5.20 and apply to the collection, maintenance and dissemination of personal data contained in manual or computerized personal data systems. Except, where otherwise provided by law or judicial order, these policies shall apply to EOEA and to any Holder of personal data as defined in these policies.

2. Definitions

In addition to the definitions set forth in M.G.L. c. 66A, s. 1, 801 CMR 3.00 et seq., and M.G.L. c. 214, ss. 1B and 3B, the following definitions shall apply to the policies set forth herein:

(A) Data Subject shall also mean any person concerning whom personal data is held for any purpose, whether or not he has knowledge of such holding.
(B) Executive Office of Elder Affairs (EOEA) means the Executive Office of Elder Affairs established by the General Court to be the principal agency of the Commonwealth to mobilize the human, physical, and financial resources available to plan, develop and implement innovative programs to insure the dignity and independence of elderly persons, including the planning, development, and implementation of a home care program for the elderly in the communities of the Commonwealth.
(C) Holder shall also mean that any agency, individual or entity which holds personal data under an arrangement, understanding or ongoing contract, or subcontract, grant or agreement with EOEA.
(D) Holds shall mean collects, maintains, or disseminates, whether manually, mechanically, or electronically. Collects shall mean gathers, obtains, or receives. Maintains shall mean stores, updates, or corrects. Disseminates shall mean transfers for any purpose from a holder to any other agency, person, or entity.
(E) Personal Data shall mean any data concerning an individual which, because of name, identifying number, mark or description can be readily associated with a particular individual; provided that such information is not contained in a public record, as defined in clause 26th of section seven of chapter four of the General Laws and shall not include

intelligence information, evaluative information or criminal offender record information as defined in section one hundred sixty seven of chapter six. (This may include, but not be necessarily limited to that which relates to the examination, care, custody, treatment, support, or rehabilitation of an individual; medical, psychological, psychiatric, social, financial, and vocational data, and which is nominally contained in case files, personnel files, or similar files). The term "personal data" shall be applied to data maintained in either manual or computerized form or any combination thereof.

(F) Personal Data System means a system of records containing personal data which system is organized such that the data are retrievable by use of the identity of the data subject.

(G) Personal Identifier shall mean any element of data which may be used to fix a person's identity either by itself or when combined with other data accessible to the holder of such data and which may include, but is not necessarily limited to: name, address, social security number, date of birth, race, zip code, mother's given name, mother's maiden name, or any letters of the mother's given or maiden name.

3. Personal Data

(A) General. Except where otherwise provided by statute, or judicial order, a holder shall not collect, maintain, or disseminate any personal data other than that which is essential for the performance of functions authorized by law. Any agency, individual or entity which holds personal data under an arrangement, understanding or ongoing contract, or subcontract, grant or agreement with EOEA on December 25, 1997 shall continue to be a Holder of Personal Data under M.G.L. c. 66A, s. 1, et seq., Executive Order 111, 801 CME 3.00, et seq. applicable regulations and section 6 of the Commonwealth Terms and Conditions for Human and Social Services on and after December 26, 1997, during the term of such agreement.

(B) Disclosure of Social Security Number. Pursuant to the Federal Privacy Act of 1974, as amended by P.L. 94-455, s. 1211, no holder shall deny to any individual any right, benefit or privilege provided by law because of the refusal by such individual to close his Social Security account number except as provided in this section. Exceptions: The previous sentence shall not apply to any disclosure which is required by federal statute; or the disclosure of a Social Security number to any holder maintaining a personal data system in existence and operating before January 1, 1975 if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(C) Identification and Assurance as Essential. A holder shall identify the kinds of personal data held and shall assure that the holding of such data is essential for the performance of functions authorized by law:

(D) Informed Consent. Each data subject may give or withhold informed consent when requested by any holder to provide personal data.

4. Administration of Personal Data

(A) Officer Designation: Each holder shall designate for each personal data system it maintains, a person to serve as the responsible person under M.G.L. c. 66A, s.2(a). A single employee may serve as the responsible person for more than one such system. He shall receive complaints and objections; answer questions; and direct operations with respect to the privacy, confidentiality, and security of personal data.

(B) Expungement of Obsolete Data. Each holder shall develop and implement a definite plan for the expungement of obsolete data with the approval of EOEA and the Records Conservation Board pursuant to M.G1. c. 30, § 42.

(C) Use of Personal Data for Unrelated Purposes. Except where otherwise provided by statute or judicial order, personal data collected for one purpose, shall not be used for another unrelated purpose without the informed consent of the data subject.

(D) Access by a Holder. A holder shall have unlimited access to personal data it holds or which is held on its behalf by another holder, provided that each holder shall permit only those employees whose duties require access to have access to personal data.

(E) Access by Non-Holders. A holder shall not allow any other entity or individual not employed by the holder to have access to personal data unless such access is authorized by statute or regulations which are consistent with the purposes of M.G.L. c. 66A, or is approved by the data subject whose personal data are sought. Medical or psychiatric data may be made available to a physician treating a data subject upon request of the physician if a medical or psychiatric emergency arises which precludes the data subject's giving approval for the release of such data.

5. Personnel Security. Each holder shall permit only those employees whose duties require access, to have access to personal data, and shall:

(A) design personnel procedures which limit the number of employees whose duties involve access to personal data;

(B) train existing personnel concerning standards of confidentially and security required by these policies;

(C) screen prospective personnel with regard to previous work experience with personal data and corresponding violations of confidentiality; and, ensure that all personnel working with or having access to personal data are familiar with M.G.L. c. 66A and pertinent regulations and policies.

6. Physical Security. Each holder shall take all reasonable steps for the protection of data from physical damage or removal, including procedures providing for:

(A) adequate fire detection and sprinkling systems;

(B) protection against water and smoke damage;

(C) alarm systems, safes and locked files, window bar, security guards or any other devices reasonably expected to prevent loss through larceny or other means of removal for manually held data, including files, tapes, cards and like materials;

(D) passwords, keys, badges, access logs, or other methods reasonably expected to prevent loss through larceny or other means of removal for mechanically or electronically held data.

(E) keeping the number of duplicate files of personal data at an absolute minimum.

(F) maintaining an audit trail of access to personal data held by it by persons or entities from outside the agency or entity.

7. Access by Data Subject

(A) Right of Access of Data Subject. Each data subject or his duly authorized representative shall have access to any personal data concerning him except where prohibited by law or judicial order. In addition, each data subject or his duly authorized representative shall enjoy the right to inspect and copy any personal data concerning him, except where prohibited. by law or judicial order.

(B) Rules Governing Access to Data. A holder may adopt reasonable written rules governing access to personal data, consistent with applicable law, regulations and these policies, which:

(1) insure that any substitute or proxy for the individual data subject be duly authorized by him;

(2) regulate the time and place for inspection and the manner and cost of copying; provided that the time for inspection shall not be unduly restricted nor shall an unreasonable cost for copying be charged; and, require that data files be reviewed in the presence of or under the supervision of the holder.

(C) Denial of Access to Data. A holder may deny a request by a data subject for access to certain personal data, such as psychiatric or psychological data, only if the denial of access is permitted by statute.

(D) Notification of Denial of Access to Data. A holder shall notify in writing an individual, in a form comprehensible to him, of its denial of his request for access, the reasons therefore, and the rights of appeal set forth in 801 CMR 3.03(3).

(E) Subpoena-Special Notice. Any holder served with a subpoena or other juducial or administrative order directing it to disseminate persoanl data, unless otherwise prohibited by law or judicial order, shall immediately give notice of such fact to the data subject to whom the data in demand relates. Such notice, where possible, shall include a copy of the order, except where the data subject himself requested the order from the issuing body or is otherwise obviously aware of its existence. Such notification must occur no later than the first business day following the day

upon which the subpoena is served. Notification shall be sent immediately by mail and include a copy of the subpoena. The holder, wherever legally and practically possible, shall allow the data subject ample time to quash the order. In addition, the holder shall attempt to reach the client (and personal representative, if known) by telephone or in person in any case where the mail might not reach him/her before the date the records production date.

The holder who accepts service of such a subpoena may wish to telephone its counsel to determine if contact with the person who caused the subpoena to be served is appropriate to determine:

1. the nature of the case;
2. whether all or some of the records described in the subpoena are truly required; and
3. whether an appearance by holder personnel may be avoided by submission of certified documents or otherwise, and if an appearance is truly necessary, narowing the scope of the subpoena to those matters truly required. The holder's legal counsel shall, as appropriate, provide additional advice or representation.

8. Monitoring and Enforcement

(A) Generally. The Secretary of EOEA or his/her designee shall be responsible for the monitoring of compliance with applicable law, regulations and these policies in cooperation with the Department of the Attorney General pursuant to M.G.L. c. 214, § 3B.

(B) Sanctions Against Employees of EOEA. Any employee of the Department of Elder Affairs found breaching the confidentiality of data subjects through violation of applicable law, regulations and these policies shall be subject to reprimand, suspension, dismissal, or other disciplinary actions by the holder consistent with any rules and regulations of the Executive Office and the Commonwealth which may govern its employees, and may be denied future access to personal data and removed from any holding responsibilities.

(C) Non-Agency Holders. Any holder, other than an agency defined under these policies, found breaching the confidentiality of data subjects through violation of applicable law, regulations and these policies shall be subject to a review and an investigation by the appropriate contracting agency of EOEA, which may lead to suspension of any contractual relationship and to legal sanctions brought by the Attorney General.

9. Agreements With Holders of Personal Data. A holder shall not allow any other person, entity or agency to hold personal data in the absence of an express contract or agreement. A holder shall assure that all contracts, subcontracts and agreements affecting the collection, maintenance or dissemination of personal data between it and any other holder of the same personal data, and a person or entity not otherwise subject to M.G.L. c. 66A, 801 CMR 3.00 et seq., or other applicable regulations and these policies, shall contain a provision requiring compliance with same.