960 CMR: OFFICE OF THE STATE TREASURER
AND RECEIVER GENERAL

960 CMR 2.00: FAIR INFORMATION PRACTICES

Section

2.01: Authority

960 CMR 2.00 is promulgated pursuant to M.G.L. c. 66A, as amended by St. 1977, c. 691.

2.02: Scope and Application

960 CMR 2.00 shall govern the collection, maintenance and disclosure of personal data contained in manual or computerized personal data systems and shall apply to the State Treasurer's Office and all agencies and boards thereunder. 960 CMR 2.00 shall not apply to criminal offender record information as defined in M.G.L. c. 6, § 167, or to personal or other data which is not contained in a personal data system.

2.03: Fees

An agency may charge a fee of ten cents per page for photocopying of records susceptible to photocopying and may charge a fee substantially equivalent to the actual cost of reproduction as determined by the responsible agency employee for copying records not susceptible to photocopying (e.g. oversize documents, punch cards or magnetic tapes).

A fee reasonably related to cost may also be charged for making a search of the system or records provided that no charge may be made for a search requiring less than one hour to complete.

2.04: Meaning of Terms

As used in 960 CMR 2.00, unless the context otherwise requires, the following terms shall have the following meanings:

Access means availability of a record to a data subject.

Agency means the State Treasurer's Office, or any board, commission or other body therein.

Data subject means an individual whose name or identity is added to or maintained in a personal data system.

Disclose means to make available or release a record to anyone other than the data subject or employees of the holding agency.

Holds means collects, maintains, or disseminates, whether manually, mechanically, or electronically.

Indexed personal data system means a personal data system from which a record may be retrieved in the ordinary course by personal identifier.

Personal data system means a collection of records a substantial number of which contain personal data or, where a record may be retrieved in the ordinary course by personal identifier, any of which contain personal data. The term does not include any collection of records containing criminal offender record information as defined in M.G.L. c. 6, § 167.

Personal identifier means 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 including, without limitation, name, address, social security number, date of birth, race or zip code.

Public records, defined in M.G.L. c. 4, § 7, par. 26, means all books, papers, maps, photographs, recorded tapes, financial statements, statistical tabulations, or other documentary materials or data, regardless of physical form or characteristics, made or received by any official or employee or an agency, unless such materials or data fall within the exemptions set out in said section 7; and, pursuant to said exemptions, shall not include materials or data specifically or by necessary implication exempted from disclosure by statute; or personnel and medical files or information, or materials or data relating to a specifically named individual, the disclosure of which may constitute and invasion of personal privacy.

2.05: Responsible Person

Each agency shall designate, for each personal data system it maintains, a person to serve as the responsible person under M.G.L. c. 66A, § 3 as amended by St. 1977, c. 691.

2.06: Duties and Responsibilities

The responsible person designated under 960 CMR 2.05 shall, with respect to the system or systems for which he is immediately responsible:

(1) ensure that the requirements of M.G.L. c. 66A and of 960 CMR 2.00 for preventing unauthorized access to or disclosure of personal data are followed;

(2) receive complaints and objection; and

(3) answer questions.

2.07: Contracts to Hold Personal Data

Agencies may enter into contracts to hold personal data but no such contract shall relieve the agency of its obligations under 960 CMR 2.00. Every such contract shall include such provisions as are necessary to ensure compliance with 260 CMR 2.00 and the Attorney General may treat the violation of any such provisions as a violation of M.G.L. c. 214, § 3B.

2.08: Personnel Training

Each agency shall inform all of its employees who have responsibilities or functions for the design, development, operation, or maintenance of a personal data system or the use of personal data therein, of the provisions of 960 CMR 2.00 and of the civil remedies described in M.G.L. c. 214, § 3B, available to individuals whose rights under M.G.L. c. 66A are allegedly violated.

2.09: Physical Security

Each agency shall take all reasonable precautions to protect personal data from fire, theft, flood, natural disaster, unauthorized removal or other security hazard.

2.10: Duplicate Files

Each agency shall keep the number of duplicate files of personal data to an absolute minimum and shall ensure that all duplicate file systems are maintained in a manner consistent with the requirements of 960 CMR 2.00.

2.11: Notice and Annual Report to the Secretary of State

Each agency shall, by April 1, 1978, and upon the subsequent establishment, termination, or change in character of a personal data system, file a report with the Supervisor of Public Records regarding each personal data system it operates in the manner prescribed below. Such report shall include, but not necessarily be limited to the following information:

(1) the name of the system;

(2) the nature and purpose of the system;

(3) the number of persons on whom data are or are expected to be maintained;

(4) the categories of data maintained, or to be maintained, indicating which categories are or will be stored in an automated personal data system;

(5) the agency's policies and practices regarding data storage, retention of data, and disposal thereof;

(6) the categories of data sources;

(7) a description of types of uses made or to be made of data, including a description of all classes of users of such data;

(8) a description of the actions taken to comply with M.G.L. c. 66A; and

(9) the name, title, and business address of the individual immediately responsible for the system.

2.12: Audit Trail

Each agency shall maintain as an audit trail records which show any disclosure of personal data the agency holds. In the case of personal data systems in which personal data

2.12: continued

is stored, in whole or in part, in a computer or in electronically controlled or accessible files, the audit trail shall include a complete and accurate record of every disclosure of personal data, including the identity of all persons and organizations to whom such disclosure has been made and their declared intentions regarding the use of the personal data disclosed. In the case of all other personal data systems, the audit trail shall include such information to the maximum extent feasible. The audit trail shall be deemed part of the data to which it relates for all purposes under 960 CMR 2.00.

2.13: Disclosure: Exception for Medical and Psychiatric Emergencies

No agency shall disclose personal data to any person or other entity unless such disclosure is authorized by state or federal statute or regulation or is approved by the holding agency and by the data subject whose personal data is sought or an authorized representative of the data subject. Medical or psychiatric data may be disclosed to a physician treating a data subject, upon the request of said physician, if a medical or psychiatric emergency arises which precludes the data subject's giving approval for such disclosure; provided, however, that the agency shall give notice of the fact of such disclosure to the data subject upon termination of the emergency.

2.14: Approval by Data Subject

The approval of a data subject or authorized representative prior to a disclosure as required by 960 CMR 2.13 may be granted in writing or orally, including by telephone; provided, that the agency seeking such approval shall make reasonable efforts to verify the identity of the data subject and the authority of any person representing the data subject; and, provided further, that the agency shall, if no written consent is given, make a notation of an oral approval and shall file such notation with the personal data held.

2.15: Disclosure of Public Records

Pursuant to M.G.L. c. 66, § 10, an agency shall disclose upon request, without consent of the data subject, any personal data which is a public record as defined in 960 CMR 2.04.

2.16: Invasion of Personal Privacy: General Rule

Personal data the disclosure of which constitute an invasion of personal privacy is not a public record. In general, it is an invasion of personal privacy under M.G.L. c. 214, § 1B, as appearing in St. 1973, c. 1114, § 72, to disclose personal data where such disclosure will result in an unreasonable, substantial or serious interference with the privacy of a data subject unless the data subject or his authorized representative consents to such disclosure.

2.17: Invasion of Personal Privacy: General Rule

In deciding whether disclosure of personal data will constitute an invasion of personal privacy, agencies shall consider the following examples:

(1) Disclosure without the consent of the data subject in the following situations is usually not an invasion of personal privacy unless the disclosure would clearly violate standards of ordinary decency:

(a) Disclosure of routine correspondence including without limitation applications for benefits under government programs;

(b) Disclosure of complaints where disclosure is accompanied by a statement as to whether any findings have been made on the complaint and what those findings are.

(2) Disclosure without the consent of the data subject which is not authorized by statute or regulation in the following situation usually is an invasion of personal privacy:

(a) Disclosure of the resume of or evaluative materials on an applicant for employment. Such materials are personnel information excluded from the definition of public records whether or not disclosure would otherwise constitute an invasion of personal privacy.

2.17: continued

(b) Disclosure of census information in any non-aggregated form which permits association of specific information with specific individuals.

2.18: Response to Compulsory Legal Process

(1) Each agency shall maintain procedures to ensure that no personal data is made available from its personal data systems in response to a demand for data by compulsory legal process unless the data subject has been notified of such demand in reasonable time to seek to have the process quashed. To fulfill this requirement, the procedures of each agency shall include:

(a) an explanation to agency personnel of rules governing the service of subpoenas in connection with proceedings before state and federal courts and administrative agencies.

(b) instructions to bring service of any subpoena immediately to the attention of the responsible person designated under 960 CMR 2.05.

2.19: Public Inquiry

Where an individual has reason to believe that personal data relating to him is held, but where the specific agency which holds such data is unknown to him, the individual may request, in writing, that the responsible person designated by the agency locate all personal data held in indexed personal data systems by agencies affected by 960 CMR 2.00. The responsible person shall make a reasonable effort to locate all such personal data and shall respond to such request within 20 days.

2.20: Right of Access

An agency shall, within 20 days of receipt of a request, grant access to any data subject, to any personal data concerning him which is held by the agency in an indexed personal data system, except where such access is prohibited by statute. In addition, such data subject shall have the right to inspect and to copy any such personal data subject to supervision.

2.21: Notification of Denial of Access to Data

An agency shall, within ten days of receipt of a request notify in writing any individual of the denial of his request for access, the reasons therefor, and the rights of appeal set forth in 960 CMR 2.24 *et seq*.

2.22: Objections by Data Subjects

A data subject who objects to the collection, maintenance, dissemination, use, accuracy, completeness or type of personal data held regarding him, may file an objection with the person responsible.

2.23: Duties of Responsible Person on Receipt of Objection from a Data Subject

On receipt of an objection, the person responsible for a data system shall investigate and if, the objection is found to be meritorious, he shall correct the contents of the data or the methods for holding or use of such data. If the objection is found to lack merit he shall allow the complainant to file and disseminate a statement of objection, accompanied by the data in question. In either event he shall notify the data subject in writing within 30 days following receipt of the objection.

2.24: Appeal of Decision of Responsible Person

Any data subject, who objects to the decision of the person responsible for the personal data system may appeal the matter to the Supervisor or Public Records. Such appeal shall be filed in writing within 30 days of notification of the decision of the person responsible for the personal data system.

2.25: Failure to Render a Decision

Any failure to render a decision at any stage of the appeal process within the time periods provided, absent contrary agreements, may be treated as a denial of the relief sought for purposes of further appeal.

2.26: Judicial Relief

No provision of 960 CMR 2.00 shall be interpreted in such a way as to preclude a data subject or the Attorney General from bringing an action in a court of proper jurisdiction in accordance with M.G.L. c. 124, § 3B.

2.27: Sanctions

Any state employee violating 960 CMR 2.00 shall be subject to reprimand, suspension, dismissal, or other disciplinary action by the employer agency consistent with the rules and regulations of the Commonwealth governing its employees.

Any agency which violates the terms of 960 CMR 2.00 may be liable to individuals injured, pursuant to M.G.L. c. 214, § 3B, and may be subject to legal action to enjoin such violations brought by the Attorney General. Any other entity which violates any provision of 960 CMR 2.00 shall be subject to a review and an investigation by the appropriate administrative agency of the State Treasurer's Office which may lead to suspension of any contractual relationship and to legal sanctions brought by the Attorney General.

2.28: Monitoring and Enforcement

The State Treasurer or his designee, shall be responsible for monitoring compliance with 960 CMR 2.00.

REGULATORY AUTHORITY

960 CMR 2.00: M.G.L. c. 66A.