950 CMR 33.00: FAIR INFORMATION PRACTICES REGULATIONS

33.01: Authority

950 CMR 33.00 is promulgated pursuant to M.G.L. c. 66A, as appearing in St. 1975, c. 776.

33.02: Scope and Application

950 CMR 33.00 shall govern the collection, maintenance and disclosure of personal data contained in manual or computerized personal data systems and shall apply to the State Secretary's Office and all agencies therein. These regulations 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. 950 CMR 3.31 shall apply to all agencies required to file notice with the State Secretary under M.G.L. c. 30 § 63.

33.03: 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 of records provided that no charge may be made for a search requiring less than one hour to complete.

33.04: Meaning of Terms

As used in 950 CMR 33.00, 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 Secretary's Office, or any board, commission or other body therein. As used in 950 CMR 3.31 the term also includes all agencies required to file notice with the State Secretary under M.G.L. c. 30, § 63.

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 as defined in M.G.L. c. 4, § 7, (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 of an agency, unless such materials or data fall within the exemptions set out in said § 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 an invasion of personal privacy.

33.05: 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, § 2(a).

33.06: Duties and Responsibilities

The responsible person designated under 950 CMR 33.05 shall, with respect to the system or systems for which he is immediately responsible:

(a) Ensure that the requirements of M.G.L. c. 66A and 950 CMR 33.00 for preventing unauthorized access to or disclosure of personal data are followed;
(b) Receive complaints and objections; and
(c) Answer questions.

33.07: 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 950 CMR 33.00. Every such contract shall include such provisions as are necessary to ensure compliance with these regulations and the Attorney General may treat the violation of any such provisions as a violation of M.G.L. c. 214, § 3B.

33.08: 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 950 CMR 33.00 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.

33.09: 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.

33.10: 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 950 CMR 33.00.

33.11: Notice and Annual Report to the Secretary of State

Each agency shall, by September 1, 1976, 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 by 950 CMR 3.31. Such report shall include, but not necessarily be limited to the following information:

(a) The name of the system;

(b) The nature and purpose of the system;

(c) The number of persons on whom data are or are expected to be maintained;

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

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

(f) The categories of data sources;

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

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

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

33.12: 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 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 950 CMR 33.00.

33.13: 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.

33.14: Approval by Data Subject

The approval of a data subject or authorized representative prior to a disclosure as required by 950 CMR 33.13 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.

33.15: Disclosure of Public Records

Pursuant to M.G.L. c. 66, § 10, an agency shall disclose upon request, without the consent of the data subject, any personal data which is a public record as defined in 950 CMR 33.04. Questions as to whether a particular record is a public record shall be resolved as provided in 950 CMR 32.00, et seq. and 950 CMR 33.16 through 33.17.

33.16: Invasion of Personal Privacy: General Rule

Personal data the disclosure of which may 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, § 62, 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.

33.17: Invasion of Personal Privacy: Examples

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:

Disclosure of routine correspondence including without limitation applications for benefits under government programs.

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 situations usually is an invasion of personal privacy:

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.

Disclosure of census information in any non-aggregated from which permits association of specific information with specific individuals.

33.18: Response to Compulsory Legal Process

Each agency shall, as required by M.G.L. c. 66A, § 2(k), 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 attempt in all cases by negotiation with the person causing the subpoena to be served to limit the scope of the subpoena to those matters truly required.

(c) A requirement that the data subject or his authorized representative be notified no later than the next business day following the day on which the subpoena is served; and

(d) A requirement that the person appearing advise the court or agency of the requirements of M.G.L. c. 66A, § 2(k).

33.19: 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 Supervisor of Public Records or his designee locate all personal data held in indexed personal data systems by agencies affected by these regulations. The Supervisor of Public Records or his designee shall make a reasonable effort to locate all such personal data and shall respond to such request within 20 days.

33.20: Request of Individual for Notification of Holding

An agency shall inform any individual in writing, upon 20 days receipt of a request, whether the agency maintains in an indexed personal data system any personal data concerning such individual.

33.21: 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 personal data to which he has access, subject to appropriate supervision. Access to personal data which is not held in an indexed personal data system and which is not prohibited by statute shall be granted by an agency to a data subject if such data subject is able to supply sufficient information to the agency to enable it to retrieve such personal data in the ordinary course.

33.22: Notification of Denial of Access to Data

An agency shall, within 10 days of receipt of a request notify in writing any individual of its denial of his request for access, the reasons therefore, and the rights of appeal set forth in 950 CMR 33.23 et seq.

33.23: 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 for the personal data system complained against. Should that person be unavailable, the data subject may make his objections to the head of the agency holding the data.

33.24: Duties of Responsible Person on Receipt of Objection

On receipt of an objection by a data subject, the person responsible for a data system shall investigate the validity of the objection. If, after the investigation, the objection is found to be meritorious, he shall correct the contents of the data or the methods for holding or the use of such data. If the objection is found to lack merit he shall provide the data subject the opportunity to have a statement reflecting views recorded and disseminated with the data in question. In either event he shall notify the data subject in writing of his decision within 30 days following receipt of the objection.

33.25: 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 of 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.

33.26: Supervisor of Public Records; Adjudicatory Hearings

The Supervisor of Public Records or his designee receiving an appeal filed pursuant to 950 CMR 33.25 shall on request of the data subject hold an adjudicatory hearing, in accordance with the provisions of M.G.L. c. 30A, within 30 days of the receipt of such appeal, and render a decision on the merits within 30 days of the conclusion of the hearing. The Supervisor of Public Records shall, within seven days of rendering a decision, notify the data subject and the person responsible for the data system of the decision and opportunities for further appeal.

33.27: Failure to Render a Decision

Any failure to render a decision at any stage of the appeal process within the time periods provided may be treated as denial of the relief sought for purposes of further appeal unless the time period has been extended by agreement between the data subject and the person required to render the decision.

33.28: Judicial Relief

No provision of these regulations 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.

33.29: Sanctions

Any employee of an agency found breaching the confidentiality of data subjects through violation of these regulations shall be subject to reprimand, suspension, dismissal, or other disciplinary actions by the employer agency consistent with the rules and regulations of the Commonwealth governing its employees, and may be denied future contact with personal data and removed from holding responsibility.

Any agency which violates the terms of 950 CMR 33.00 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 entity other than an agency which violates any provision of these regulations shall be subject to a review and an investigation by the appropriate administrative agency of the State Secretary's office which may lead to suspension of any contractual relationship and to legal sanctions brought by the Attorney General.

33.30: Monitoring and Enforcement

The State Secretary, or his designee, shall be responsible for monitoring compliance with these regulations in cooperation with the Office of the Attorney General pursuant to M.G.L. c. 214, § 3B.

33.31: Filing of Notice Required by M.G.L. c. 30, § 63

All agencies required to file notice with the State Secretary under M.G.L. c. 30, § 63, shall do so on a form approved by the Supervisor of Public Records which form shall be attached to a be a part of 950 CMR 33.00.

33.32: Personal Data System

Form 1.

The following information is required to be filed with the State Secretary for compliance with the Fair Information Practices Act.

AGENCY: _____ EXECUTIVE OFFICE _____

PERSON RESPONSIBLE FOR SYSTEM: _____

TITLE: _____ BUSINESS ADDRESS: _____

SYSTEM NAME: _____

NATURE AND PURPOSE OF SYSTEM: _____

_____

CATEGORIES OF DATA; NUMBER OF DATA SUBJECTS WITHIN CATEGORIES: _____

IS SYSTEM AUTOMATED: YES _____ NO _____ PARTIALLY _____

IF AUTOMATED OR PARTIALLY SO, DESCRIBE: _____

METHODS OF STORAGE: _____

RETENTION AND DISPOSITION SCHEDULES: (as approved by the Records Conservation Board)_____

CATEGORIES OF DATA SOURCES: _____

CATEGORIES OF DATA ELEMENTS: _____

33.32: continued

Form 1. (continued)

USES OF DATA AND DESCRIPTION OF CLASSES OF USERS:_____

DISCLOSURES OUTSIDE AGENCY: _____

ACTIONS TAKEN TO COMPLY WITH CHAPTER 66A: _____

SIGNATURE _____

REGULATORY AUTHORITY

950 CMR 33.00: M.G.L. c. 66A.