760 CMR 8

760 CMR 8.00:

PRIVACY AND CONFIDENTIALITY

8.01: Applicability and Definitions

760 CMR 8.00 shall be effective on November 15, 1996. 760 CMR 8.00 replaces prior regulations appearing at 751 CMR 7.00.

The definitions of data subject, personal data, and personal data system appear in M.G.L. c. 66A, § 1. In addition, the following definitions apply:

Department - the Massachusetts Department of Housing and Community Development.

Holder - A local housing authority, redevelopment authority and any other person or entity which has a written contract, agreement or arrangement with a local housing authority or redevelopment authority to hold personal data in performing a governmental or public function or purpose.

LHA - a local or regional housing authority established under M.G.L. c. 121B, § 3 or § 3A, or a comparable special act.

LRA - a local redevelopment authority established under M.G.L. c. 121B, § 4.

8.02: Informed Consent

A data subject may give or withhold informed consent when requested by a holder to provide personal data.

(1) Written Statement from Holder. Consent will be deemed "informed consent" only if the holder provides to the data subject a written statement containing the following information and the data subject indicates his/her written understanding and agreement:

(a) an explanation of how the requested data will be used and held;

(b) the identity of persons, entities or agencies who will receive or hold the data, and an assurance that all holders will keep the data confidential;

(c) an offer to answer any inquiries concerning the data, indicating the data subject's right to object in accordance with 760 CMR 8.05; and,

(d) any legal requirements to provide the requested data and any legal or administrative consequences arising from a decision to withhold the data.

(2) Separate Approval for Data Use. 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.

8.03: Collection and Maintenance of Personal Data

(1) Designation of Personal Data Officer. Each LHA and LRA shall designate one individual to serve as the officer immediately responsible for the privacy, confidentiality, and security of personal data consistent with M.G.L. c. 66A.

(2) Limit on Personal Data. A Holder shall not collect or maintain more personal data than reasonably necessary for the performance of the holder's legally authorized functions.

8.04:: Access to Personal Data

(1) Contracts or Agreements with a Holder to Perform a Public or Governmental Purpose. A LHA or LRA shall allow another person, entity or agency to hold personal data for a governmental function or purpose only by written contract, agreement, or arrangement. Such contract, agreement, or arrangement shall contain provisions expressly informing the other person, entity or agency of its status as a Holder and covering its legal obligations as such.

(2) Dissemination of Personal Data - General. A Holder shall not allow any individual, agency, or entity not employed by the Holder or under contract or agreement with the Holder under 760 CMR 8.04(1) to have access to personal data unless such access is:

(a) authorized by statute or by regulations which are consistent with the purposes of M.G.L. c. 66A; or

(b) approved by the data subject, unless the data subject is not entitled to access.

(3) Access by Physicians in an Emergency. A Holder may disseminate medical or psychiatric data to a physician treating a data subject, upon the request of the physician, if a medical or psychiatric emergency arises precluding the data subject from approving the release of the data. Upon termination of the emergency, the Holder shall give notice to the data subject about the physician's access.

(4) Access by the Department. A Holder shall permit authorized employees of the Department to have access to personal data for the performance of legally authorized duties and responsibilities and shall disseminate personal data to the Department upon its request.

(5) Access by Holder Personnel and Board Members. A Holder shall:

(a) design personnel procedures which limit the number of employees whose duties involve access to personal data and train existing personnel concerning standards of confidentiality and security required by 760 CMR 8.00;

(b) permit only those employees whose duties require access to have access to personal data; and

(c) strictly limit board member access to personal data concerning an applicant or tenant to situations where there is a need for access in order for the board to conduct business properly.

(6) Access bevy Data Subject. A data subject or his/her duly authorized representative shall have access to, as well as the right to inspect and copy, any personal data concerning him/her, unless prohibited by law or judicial order.

(7) Denial of Access to Data Subject. A Holder shall not rely on any exception contained in M.G.L. c. 4, § 7 clause twenty-sixth (public records law) to withhold personal data from a data subject. A Holder may deny a request by a data subject or his/her authorized representative for access to personal data if:

(a) the denial of access is expressly permitted by statute; or

(b) the personal data is currently the subject of an investigation and its disclosure would probably so prejudice the possibility of effective law enforcement that the disclosure would not be in the public interest. 760 CMR 8.04(7) is not intended to limit any right or power of access the data subject might have under pertinent administrative or judicial procedures. Such personal data may be withheld for the time for completion of the investigation and commencement of an administrative or judicial proceeding on its basis, or for one year from the commencement of the investigation, whichever occurs first.

(8) Notice of Denial. A Holder shall notify a data subject in writing of any denial of his/her request for access, the reasons therefore, and the right of appeal set forth in 760 CMR 8.05.

(9) List of Data Requests. A Holder shall, at the request of a data subject, provide a written list of the uses made of his/her personal data, including any persons, agencies, or entities which have gained access to the personal data.

(10) Holder Authority to Make Additional Access Rules. A Holder may adopt reasonable written rules governing access to personal data, consistent with 760 CMR 8.00 and all pertinent statutes which:

(a) insure that any substitute or proxy for the data subject be duly authorized by him/her;

(b) 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, and the fee for copies shall not exceed that allowed for public records under the Freedom of Information regulations of the Massachusetts Supervisor of Public Records; and

(c) require that data be reviewed in the presence of or under the supervision of the Holder.

(11) Judicial or Administrative Orders. Any Holder served with a subpoena or other judicial or administrative order directing it to disclose a data subject's personal data shall, unless otherwise prohibited by law or judicial order, immediately give notice to the data subject. Such notice, where possible, shall include a copy of the subpoena or order, except where the data subject himself requests the order or is otherwise obviously aware of its existence. The holder, wherever legally and practically possible, shall allow the data subject adequate time to attempt to secure a court order to quash the subpoena or order.

(12) Record of Data Access and Use. Each Holder shall maintain a complete and accurate record of every access to any personal data by persons, agencies, or entities other than the holder, including the identity of all such persons, agencies, and entities and their intended use of the data.

(13) Physical Safety of Data. A Holder shall take all reasonable measures to protect personal data from physical damage or removal.

8.05: Objections and Administrative Appeals

(1) Data Subject's Right to Object. A data subject who objects to the accuracy, completeness, pertinence, timeliness, relevance, use, or dissemination of his/her personal data or the denial of access to his/her personal data, may personally, or through a duly authorized representative, file an objection with the personal data officer.

(2) Meritorious and Non-meritorious Objections. The personal data officer shall investigate the validity of the objection within 30 days of receipt and

(a) if the objection is found to be meritorious, he or she shall correct or amend the data or the methods for the use or dissemination of the data, or as appropriate, permit access by the data subject to the data; or

(b) if the objection is found to lack merit, provide the data subject the opportunity to have a statement reflecting his/her views recorded and included with any subsequent dissemination of the personal data in question.

(3) Data Subject Appeal. Any data subject, including an applicant or tenant, or his/her authorized representative may appeal the personal data officer's decision pursuant to the LHA or LRA grievance procedures.

8.06: Administration and Enforcement

(1) Data System Notices to Secretary of State. Each Holder shall upon the establishment, termination, or change in the character of a personal data system, file a notice with the Massachusetts Secretary of State pursuant to M.G.L. c. 30, § 63.

(2) Departmental Power of Review. The Department may from time to time review the procedures of a Holder under 760 CMR 8.00. If the Department finds the procedures deficient, the Department shall direct corrective measures.

(3) Legal Action. Any Holder which violates a provision of M.G.L. c. 66A may be subject to legal action pursuant to M.G.L. c. 214, § 3B.

REGULATORY AUTHORITY

760 CMR 8.00: M.G.L. c. 66A; c. 30, §3; c. 214, § 3B and Mass. Exec. Order No. 111 - Fair Information Practices.