610 CMR 10.00: Privacy, Confidentiality, and Data Security

10.01: General Provisions

(1) Scope and Purpose. The Board of Higher Education pursuant to St. 1996, c. 151, continues 610 CMR 10.00 in full force and effect, unless the boards of trustees of the public institutions under the Board of Higher Education have promulgated or adopted privacy, confidentiality, and data security regulations applicable to their institutions. Additionally regulations previously promulgated as 610 CMR 4.00 pursuant to M.G.L. c. 15A, § 9(s) have been merged into 610 CMR 10.00. Except where otherwise provided by law or judicial order, the provisions of 610 CMR 10.00 shall apply to the collection, maintenance, security, and dissemination of personal data contained in manual or computerized personal data systems and educational data collected by the Board of Higher Education.

610 CMR 10.00 shall not apply to:

(a) criminal offender record information as defined in M.G.L. c. 6, § 167;

(b) intelligence, analytical or investigative criminal reports, criminal evaluative data to the extent that the disclosure of such to a data subject would endanger the life or well-being of any person;

(c) personal data or other data which is not contained in a personal data system, or collected as educational data by the Board of Higher Education from public and independent institutions of higher education and other institutions, organizations and entities holding or otherwise involved with such data; and

(d) public records as otherwise defined in M.G.L. c. 4, § 7(26).

(2) Application to the Board of Higher Education and Public Institutions of Higher Education. Except where otherwise provided by law or judicial order, 610 CMR 10.00 shall apply to the Board of Higher Education and all public institutions of higher education.

10.02: Definitions

For the purposes of 610 CMR 10.00, the following terms will mean:

Agency. The Commonwealth or any of its departments, authorities established by the General Court to serve a public purpose having either state-wide or local jurisdiction, boards, and commissions, or other entities, except criminal justice agencies as defined in M.G.L. c. 6, § 167, to the extent described in 610 CMR 10.01(2).

Audit Trail. A recording by a holder of all persons who obtain access to the personal records of a data subject.

Board of Higher Education (Board). The Agency established by M.G.L. c. 15A, § 4 and all of its divisions.

Commissioner of the Board of Higher Education (Commissioner). The chief executive and administrative officer of the Department of Higher Education and Board of Higher Education, pursuant to M.G.L. c. 15A, § 6.

Collects. Gathers, obtains or receives.

Data Subject. Any person concerning whom personal data is held for any purpose, whether or not he has knowledge of such holding.

Data Security. Reasonable precaution from unauthorized access, theft, removal or other security threat.

Directory Information. May include an individual's name, address, telephone number, date of birth, place of birth, major field of study or employment position, participation in officially recognized activities and sports, name of institution, weight and height of members of the athletic team, dates of attendance, degree and awards received, the most recent previous educational agency or institution attended by the student, or other similar information. The Board may, at its option, define certain data as Directory Information to include the data described above; provided, however, that nothing contained in 610 C MR 10.00 shall require the Board to disclose individualized personal data not otherwise exempt by applicable federal or state law.

Disclosure. Access or release of data:

(a) Access - inspection or copying of data or reports generated therefrom.
(b) Release - the written disclosure, in whole or in part, of data or reports generated therefrom.

Disseminates. Transfers for any purpose from a holder to any other agency, person, or entity.

Educational Data. All available educational data, aggregate and individualized, collected from data holders on paper, magnetic tape and/or in computerized or electronic form, relevant to the careful and responsible discharge of the purposes, functions, and duties of the Board.

Holder. Any agency to which 610 CMR 10.00 applies pursuant to 610 CMR 10.01(2) and as defined in 610 CMR 10.02 and any other person or institution, organization or other entity that holds or is involved in the aggregation, maintenance of personal data.

Holds. Collects, maintains, or disseminates, whether manually, mechanically, or electronically.

Independent Institution o f Higher Education. Any degree-granting institution of higher educationlocated or offering degree programs or courses in Massachusetts excluding public institutions of higher education set forth in M.G.L. c. 15A, § 5.

Institution under the Board of Higher Education. Any institution within the system of public institutions of higher education as set forth in M.G.L. c. 15A, § 5.

Individual. A student or employee:

(a) Student - any person enrolled or formerly enrolled in an institution of higher education in Massachusetts.

(a) Employee - any person (faculty, administrative, or support staff) employed by an institution or other data holder including faculty, administrative or support staff.

Legal Proceeding. Any litigation, arbitration, or state or federal administrative proceeding.

Maintains. Stores, updates, or corrects.

Official Data. Standard reports prepared and released by the Board in consultation with appropriately involved institutions or other data holders. The Board and the institutions shall rely upon this data in public statements and reports wherever reasonably practicable. Official data shall not contain individualized data unless or until the Board, at its option, designates certain data as Directory Information following consultation with each institution.

Personal Data. Any data regarding an individual including but not limited to personal identifiers, which relate to the examination, care, custody, treatment, support, or rehabilitation of the individual, medical, psychological, psychiatric, social, financial, and vocational data, and which is normally contained in case files, personnel files, or similar files. The term "personal data" shall be applied to data maintained in either manual or computerized or electronic form or any combination thereof.

Personal Data System. A collection of records, a substantial number of which contain personal data, where access to the records can be gained by the use of a personal identifier.

Personal Identifier. Any element or 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.

10.03: Collection, Maintenance, and Dissemination of Personal Data

(1) Personal Data:

(a) General. Except where otherwise provided by statute, regulation, 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.

1. Administration. Acting pursuant to applicable provisions of M.G.L. c. 15A, the Board is legally responsible for providing certain aggregate educational data in report form to the legislative and executive branches of the Commonwealth and to the public. This aggregate data which shall be available for dissemination shall be produced in standard reports, including but not limited to enrollment, program inventory, regular statistical reports, special studies, tuition and fees, and enrollment projections. Such reports shall be prepared, issued or released on a regular schedule and upon executive or legislative request.

2. Release of Official Data. The Board shall prepare and have available certain aggregate educational data for release through public statements and in standard report format whenever reasonably practicable. Such data may be contained in regular statistical reports, special studies, testimonies or public statements. Data releases that do not conform to established Board's available standard report format(s) shall meet Board's internal standards to assure that they are current, consistent with other sources, and supported by adequate background information and analysis.

3. Accuracy of data. The Board shall take reasonable steps to ensure that all educational data collected from data holders is accurate, complete and consistent with data previously on file with the Board or provided to the Board by other data holders. Data or reports prepared by the Board for disclosure which do not conform to the established Board's standard report format(s) shall be accurate, current and consistent with their sources, and shall, whenever practicable, be supported by adequate background information and analysis.

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

1. prior to the inception of any personal data system, notices should be published in generally read newspapers in all communities in the Commonwealth, through all other reasonable means of drawing attention to such data held;

2. statements of identification of kinds of data held and assurance should be recorded in an individual file accessible to periodic examination by the Commissioner or his designee and the inclusion of such statements in the notice and annual report to be submitted pursuant to 610 CMR 10.03(2)(f);

3. to the extent possible, at the time of collection of data within the context of informed consent procedures conducted pursuant to 610 CMR 10.04(3) and 10.04(4).

(c) Review by the Commissioner. The Commissioner or his designee may review the procedure of any institution relating to the conformance with 610 CMR 10.00. If the Commissioner or his designee should find that any institution or Board employee is not conforming to the procedures set forth in 610 CMR 10.00 the Commissioner may direct the chief executive officer of the institution or the Board's employee's supervisor to arrange for compliance forthwith. The Commissioner shall report further violations to the Attorney General for action pursuant to M.G.L. c. 214, § 3B.

(d) Public inquiry. Where an individual has reason to believe that personal data relating to him is held, but where the specific holder of such data is unknown to him, the Commissioner or his designee upon written request from the individual, shall within 30 days make every reasonable effort to locate all such personal data held by the Board of Higher Education or the institutions affected by 610 CMR 10.00.

(e) Holder agreements. All institutions and the Board of Higher Education holding personal data shall assure that all agreements affecting the collection, maintenance, or dissemination of personal data established between a holder and a person or entity not otherwise subject to 610 CMR 10.00 shall contain provisions requiring compliance with 610 CMR 10.00. Where agreements are absent, institutions and the Board of Higher Education shall arrange for the development of such to require compliance with 610 CMR 10.03.

(2) Administration of Personal Data.

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

(b) Use of personal data for unrelated purposes. Except where otherwise provided by statute, regulation 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 pursuant to 610 CMR 10.04(3) and 10.04(4).

(c) Personnel Security. Each holder shall permit only those employees whose duties require access, to have access to personal data, and shall: design personnel procedures which limit the number of employees whose duties involve access to personal data; train existing personnel concerning standards of confidentiality and security required by 610 CMR 10.00; 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 regulation, or

is approved by the holder and by the data subject; 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 610 CMR 10.00, the provisions of M.G.L. c. 66A, M.G.L. c. 30, § 63, and M.G.L. c. 214, § 3B, and other pertinent legislation.

(d) Physical security. Each holder shall take all reasonable steps for the protection of data from physical damage or removal, including procedures providing for: adequate fire detection and sprinkling systems; protection against water and smoke damage; watertight facilities; alarm systems, safes and locked files, window bars, 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; and, 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) Duplicate files. Each holder shall insure that the number of duplicate files of personal data is maintained at an absolute minimum. Each holder shall insure that any duplicate file systems are maintained consistent with the requirements of 610 CMR 10.00.

(f) Notice and annual report to the Commissioner of the Board of Higher Education. Each holder shall annually and upon the subsequent establishment, termination, or change in character of a personal data system file a report with the Commissioner regarding each personal data system it operates. Such reports shall include, but not necessarily be limited to the following information: the name of the system and the title and address of the person in charge of it, the nature and purpose of the system, the identification of the types, categories, uses and sources of data held in the system and the assurance that such data is essential, pursuant to 610 CMR 10.03(1)(b), the approximate number of individuals about whom data is held in the system, whether and to what extent the data is held in computerized form, a description of each person and organization having access to the system; a description of the policies and practices of the holder with regard to data maintenance, retention, and disposal, a description of the manner in which any individual who believes that the data about him is held in the system may have a search made, and, if such data is so held, may inspect, copy, and object to it as provided in 610 CMR 10.00; and a description of other actions take to comply with 610 CMR 10.00 and Massachusetts Law, particularly M.G.L. c. 66A, a statement that this report is available upon request in compliance with 610 CMR 10.00.

(g) Audit trail. Each holder shall maintain the most feasibly precise records of having access to and the uses of the personal data it holds, consistent with the following requirements:

1. where such data is held in computerized form, the data system shall have the capacity for a program or programs to electronically record all persons collecting, examining or using data and purposes of such collection, examination, or use.

2. where the data is held in manual form, the holder shall require that a manual notation be made, to the maximum extent possible, of all persons collecting, examining or using data and the purposes of such collection, examination, or use.

3. the audit trail developed shall all be deemed part of the data held, and shall thereby be accessible only to the following persons: the data subject or his authorized representative, individuals authorized to have access in accordance with 610 CMR 10.03(2)(c), and, the Commissioner or his designee for purposes of reviewing and monitoring compliance with 610 CMR 10.00.

4. in cases where a room is maintained solely for the purpose of holding data, the holder shall maintain a log which records the names of persons having access to the room. Where a room is not maintained solely for that purpose, the holder shall maintain a log which records the names of persons actually working with such data, and the dates and lengths of time of such use.

(h) Periodic review of personal data held. Each holder shall, at least once every 24 months, review its personal data system(s) with respect to the accuracy, current need, relevance, and timeliness of data held, and shall adhere to the following provisions:

1. each holder shall adopt a written plan for such review, describing the systems involved, the schedule for such review, and the persons making the review. Each holder shall submit such review plan to the Commissioner or his designee. The plan as approved shall be a public record;

2. immediately following the completion of such a review, the persons who conducted the review shall make a written report describing the files, tapes, records, films or data reviewed and the degree of conformance by the holder with 610 CMR 10.00; and

3. a copy of the report shall be submitted to the chief executive officer of the institution and the Commissioner along with any suggestions as to whether any changes to 610 CMR 10.00 should be considered.

(i) Holding -- notice to Secretary of State. The holders of personal data shall comply with the requirements of M.G.L. c. 66A, § 2.

(j) Dissemination -- notice to subsequent holders. Each holder, when disseminating personal data, shall insure that any subsequent holder is aware of the requirements of 610 CMR

10.00, M.G.L. c. 66A, M.G.L. c. 30, § 63, and M.G.L. c. 214, § 3B, other pertinent statutes, Executive Order No. 111 (Fair Information Practices), and any written policy directives developed by such agency relating to the use of such data, and shall take all reasonable steps to assure that such data is used only in accordance with such mandates.

(k) Objection by data subject -- dispensing holding activities. A data subject may file an objection with a holder regarding procedures for holding data or the types of data held, in accordance with 610 CMR 10.04(2) through 10.04(16). During the pendency of any objection, except where otherwise provided by law or judicial order, the holder in question shall make all reasonable attempts to dispense with any further holding activities beyond mere storage, relating to the particular data in question, until such objection has been resolved.

(l) Master plan. Each holder, prior to the computerization or automation of any existing personal data system and prior to the initial development of any new manual or computerized system, shall establish in writing a master plan containing the following elements:

1. identification and justification of personal data as essential in accordance with 610 CMR 10.03(1);

2. brief descriptions of existing or planned agreements involving the holding of personal data in accordance with 610 CMR 10.03(1)(e).

3. statements reflecting proposed action on and compliance with each of the mandates presented in this part, particularly, the provision of an annual report and a written plan for periodic review of data held, in accordance with 610 CMR 10.03(2)(f) and 10.03(2)(h) herein; and

4. the identification of foreseeable threats to the security of personal data held, and a corresponding description of all measures to be employed as safeguards designed to avoid or mitigate such threats, including but not necessarily limited to, plans involving personnel training relating to data system operations and 610 CMR 10.00.

(m) 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 regulation, or is approved by the holder and by the data subject whose personal data is held.

(n) Subpoena – special notice. Any holder served with a subpoena or other judicial or administrative order directing it to disseminate personal data, unless otherwise prohibited by law or judicial order, shall immediately give notice of such fact to the data subject. Such notice, where possible, shall include a copy of the order, except where the data subject is the moving party or is otherwise obviously aware of its existence. The holder,

wherever legally and practically possible, shall allow the data subject ample time to seek to quash the order prior to complying with the order.

(o) Funding applications. Any holder applying for a loan, grant, contract or appropriation to fund a project involving the holding of personal data in a personal data system shall include in such application a funding request for financing the protection of the privacy of personal data and for compliance with 610 CMR 10.00.

(p) Legal Proceeding Exception.

1. Where a suit (or legal proceeding) has been threatened or instituted by a data subject against the Commonwealth, the Board of Higher Education, division, or public institution of higher education, or against any official employee of the Board or a public institution of higher education, arising from his or her official duties or scope of employment, any personal data concerning the data subject, held by the entity that is or employs a party to such suit (or legal proceeding), which is relevant to a determination of the issues in dispute, shall be furnished to the Attorney General, or authorized assistant attorney general or special assistant attorney general who may further disclose such personal data to the extent he or she deems necessary for purposes of representing the defendant(s), subject to the following conditions:

    a. disclosure shall be furnished in response to a written or oral request from the office of the Attorney General which shall indicate the purpose of which the personal data is requested and describe, with particularity, the data requested; and

    b. personal data of persons not a party of the litigation (or legal proceeding) will be redacted in order to protect the privacy interests of such persons.

2. In the event that a personal data system maintained by the Commonwealth, Board of Higher Education or public institutions of higher education, to carry out its functions, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising under a statute, rule, regulation or order issued pursuant thereto, the relevant data may be referred to the Attorney General in order to enforce or implement the statute, rule, regulation or order issued pursuant thereto, or to investigate or prosecute such violation.

3. Nothing in 610 CMR 10.03 shall be construed to authorize the Board of Higher Education or Public institutions of higher education to release information, the disclosure of which is prohibited by any statute other than the Fair Information Practices Act, M.G.L. c. 66A.

(3) Enforcement.

(a) Employees of the Board of Higher Education or of institutions under the Board of Higher Education:

1. Any employee at the Board of Higher Education or at a public institution of higher education found breaching the confidentiality of data subjects through violations of 610 CMR 10.00 shall be subject to reprimand, suspension, dismissal or other disciplinary actions by the holder, the chief executive officer of the institution, the Board of Higher Education and the Commonwealth governing its employees, and may be denied future access to personal data and removed from any custodial responsibilities.

2. The Board of Higher Education or any institution under the Board of Higher Education or any institutions which violates the terms of 610 CMR 10.00 may be liable to individuals injured, pursuant to M.G.L. c. 214, § 3B, to legal action to enjoin such violations brought by the Attorney General, and to administrative action by the institution or the Board of Higher Education to remove authorization to hold personal data.

(b) Non-agency holders: Any holder, other than defined under 610 CMR 10.02, found breaching the confidentiality of data subjects through violation of 610 CMR 10.00 shall be subject to a review and an investigation by the appropriate contracting agency which may lead to suspension of any contractual or licensure relationship and to legal sanctions brought by the Attorney General.

(c) Monitoring and Enforcement. The Commissioner shall be responsible for the monitoring of compliance with 610 CMR 10.00 in cooperation with the Department of the Attorney General pursuant to M.G.L. c. 214, § 3B.

10.04: Individual Rights and Safeguards

(1) Information Officers: Officer Designation. Each holder, as defined under 610 CMR 10.02, shall designate one person to serve as the officer responsible for any personal data system maintained by such holder.

(2) Duties and Responsibilities of Information Officers. The officer described in 610 CMR 10.04(1) shall insure that all data subjects enjoy the rights provided under 610 CMR 10.00, and under M.G.L. c. 66A, M.G.L. c. 30, § 63, and M.G.L. c. 214, § 3B, and he shall receive complaints and objections, answer questions, and direct operations with respect to the privacy, confidentiality, and security of personal data.

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

(4) Criteria for Informed Consent. Consent may be deemed to be "informed consent" only if the holder provides the following information to the data subject and the data subject indicates his understanding and agreement:

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

(b) a statement identifying the agencies or persons who are likely to receive or hold the data, and an assurance that all such holders will keep the data confidential;

(c) an offer to answer any inquiries concerning the methods of holding data and the types of data to be held, with a statement indicating the right of a person to object to such methods or types in accordance with 610 CMR 10.04(12) through 10.04(16); and

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

(5) Request on Data. A holder, upon request of an individual, shall inform the individual in writing and in a form comprehensible to him or her whether such holder maintains, holds, or has held any personal data concerning him or her within the previous 24 months.

(6) Statement of Rights. A holder shall furnish to any person requested to provide personal data a statement listing all individual rights set forth in 610 CMR 10.00.

(7) Emergencies. A holder may disseminate medical or psychiatric data 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 from giving approval for the release of such data; provided, however, that the data subject shall be given notice of such access upon termination of the emergency.

(8) Right of Access of Data Subject. Each data subject or his duly authorized representative shall, upon request, 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 held concerning him except where prohibited by law or judicial order.

(9) Access to Data by Data Subject. A holder may adopt reasonable written rules governing access to personal data, consistent with 610 CMR 10.00 and all pertinent legislation, which:

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

(b) regulate the time and place for inspection and the manner and cost of copying. The time for inspection shall not be unduly restricted nor shall any unreasonable cost for copying to be charged; and

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

(10) Denial of Access to Data. A holder may deny a request by a data subject for access to personal data, which consists of psychiatric or psychological date, only if the denial of access is permitted by statute.

(11) Notification of Denial of Access to Data. A holder shall notify in writing any individual of its denial of his or her request for access, the reasons therefore, and the rights of appeal set forth in 610 CMR 10.04(12) through 10.04(16).

(12) Objection by the Individual. An individual whose educational or personal data is held by the Board may contest the accuracy, completeness, pertinence, timeliness or relevance of the data, or its dissemination or access to third parties. Such objection shall be in writing and filed with the data holder for its administrative review, investigation and final determination.

(13) Responsibilities of Holder Pursuant to Objection. Pursuant to an objection by a data subject, the officer responsible for a data system shall within 30 days of the receipt of the objection:

(a) notify, in writing, the appropriate agency head under whose authority personal data is held regarding the nature of the objection;

(b) investigate the validity of the objection. If, after the investigation the objection is found to be meritorious, correct the contents of the data or the methods for holding or the use of such data; or, if the objection is found to lack merit, provide the data subject the opportunity to have a statement reflecting his views recorded and disseminated with the data in question;

(c) notify, in writing, the appropriate chief executive officer of the institution or Commissioner of the Board of Higher Education under whose authority personal data is held regarding the action taken; and

(d) notify in writing the data subject of the outcomes of the investigation.

(14) Appeal of Holder's Decision. Any data subject, who objects to the decision of the officer in charge of the personal data system may appeal the matter to the chief executive officer of the institution or the Commissioner of the Board of Higher Education under whose authority the

personal data in question is held. Such appeal shall be filed in writing within 30 days of notification of the decision by the officer in charge of the personal data system.

(15) Chief Executive Officer of the Institution or the Commissioner of the Board of Higher Education; Adjudicatory Hearing. A chief executive officer of the institution or the Commissioner of the Board of Higher Education hearing an appeal filed pursuant to 610 CMR 10.04(14) shall:

(a) at the written request of the appellant data subject convene 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 said hearing;

(b) notify, in writing, the Commissioner of the Board of Higher Education within seven days of the receipt of such appeal, regarding the nature of and filing of the appeal; and, within seven days of rendering a final decision on the merits, notify the appellant data subject and the appellee holder regarding the nature of the decision.

(16) Failure to Render a Decision. Any failure to render a decision at any stage of the appeal process within the time periods set out in this part shall result in a decision favorable to the appellant data subject, except that the time periods may be extended by agreement between the data subject and the holder.