VOTE
ON
FAIR INFORMATION PRACTICES REGULATIONS

VOTED: To rescind the vote of the Board of Trustees on August 4, 1976, approving and adopting the University's Interim Privacy and Confidentiality Regulations (Doc. T77-005), and to approve and adopt in place thereof the University Fair Information Practices Regulations (Doc. T77-059); further, to direct the campuses and the President's Office to prepare and publish simplified guidelines for the implementation of the Regulations and for informing individuals of their rights and responsibilities under the Regulations.

Approved by the Board of Trustees 2/2/77
UNIVERSITY OF MASSACHUSETTS
FAIR INFORMATION PRACTICES REGULATIONS

Part I - General Provisions

§101 Authority

These regulations are promulgated pursuant to the provisions of G.L. c. 75, §§1 & 3, and the requirements of G.L. c. 66A, as inserted by St. 1975, c. 776.

§102 Scope and Purpose

Except where otherwise provided by law or judicial order the provisions of these regulations shall apply to the collection, maintenance, and dissemination of personal data contained in manual or computerized personal data systems. These regulations shall not apply to:

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

(b) intelligence, analytical, or investigative criminal reports or criminal reports or 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 are not contained in a personal data system;

(d) public records as defined in G.L. c. 4, §7 or public information as defined in §103(c) of these regulations; or

(e) hospital records subject to the provisions of G.L. c. 111, §70

In addition, these regulations shall not apply to confidential letters and statements of recommendation or evaluation received prior to July 1, 1976, provided, that such letters and statements were solicited under a written assurance of confidentiality, or were sent or retained with a verifiable understanding of confidentiality, and provided, further, that they are being used solely for the purposes for which they were specifically intended.
If any of these regulations should conflict with applicable provisions of the federal Family Educational Rights and Privacy Act of 1974 (section 438 of the General Education Provisions Act, added by section 513 of Pub. L. 93-380 and amended by section 2 of Pub. L. 93-568), or of any regulations promulgated pursuant to said act, the provisions of said federal act or federal regulations shall control.

§103 Definitions

(a) "Audit Trail"

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

(b) "Board"

"Board" shall mean the Board of Trustees of the University of Massachusetts.

(c) "Campus" and "Campus Head"

"Campus" shall mean, depending on its context, the University of Massachusetts at Amherst, the University of Massachusetts at Boston, or the University of Massachusetts at Worcester, including all constituent colleges, schools, departments, agencies, institutes or stations, wherever located, under the general superintendence of the campus Chancellor. Unless the context clearly indicates otherwise, "campus" shall also include the Office of the President of the University. The term "campus head" shall mean the Chancellor or the President, as the case may be.

(d) "Collects"

"Collects" shall mean gathers, obtains or receives.

(e) "Data Subject"

"Data Subject" shall mean any person concerning whom personal data is held for any purpose, whether or not he has knowledge of such holding.
"Directory Information"

"Directory Information" shall mean the following information relating to a data subject: name, University and home address and telephone number, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance at the University, degrees and awards received, the most recent educational institution attended by a student or any such institution attended by or having employed a faculty or staff member, and other similar information. "Directory Information" shall not include that information included in the definition of "public information" in subsection (c) of this section.

"Disseminates"

"Disseminates" shall mean transfers for any purpose from a holder to any other agency, person or entity.

"Holder"

"Holder" shall mean any campus to which these regulations apply and any other person or entity who or which enters into a contract or other agreement with such campus to hold personal data.

"Holds"

"Holds" shall mean collects, maintains, or disseminates, whether manually, mechanically, or electronically.

"Hospital Records"

"Hospital Records" shall mean records of the treatment of cases under the care of the teaching hospital at Worcester or of the health services at Amherst and Boston, including the medical history and nurses' notes, as provided in G.L. c. 111, §70.

"Maintains"

"Maintains" shall mean stores, updates, or corrects.

"Personal Data"

"Personal Data" shall mean any data regarding an individual including personal identifiers, and including, but not necessarily limited to those which relate to the examination, care, custody,
treatment, support, or rehabilitation of the individual, medical, psychological, psychiatric, social, financial, and vocational data, and which are 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 form or any combination thereof but shall not include "public records" defined in G.L. c. 4, §7, or hospital records subject to the provisions of G.L. c. 111, §70.

"Personal Data System"

"Personal Data System" shall mean a collection of records containing personal data, but shall not include: criminal offender record information, as defined in G.L. c. 6, §167; intelligence, analytical and investigative criminal reports, and criminal evaluative data as described under §102(b) herein; personal data or other data, otherwise qualifying as personal data under §103(l) herein, not contained in a personal data system; public records as defined in G.L. c. 4, §7; or hospital records subject to the provisions of G.L. c. 111, §70.

"Personal Identifier"

"Personal Identifier" shall mean any element of data which may be used to fix a person's identity either by themselves or when combined with other data accessible to the holder of such data and which may include, but 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.

"Public Information"

"Public Information" shall mean, in the case of any employee of the University, the following: name, position title, job description, salary, office location and telephone number and dates of employment at the University.

"Public Records"

"Public Records" shall mean 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 officer or employee of any agency, executive office, department, board, commission, bureau, division or authority of the Commonwealth, or any political subdivision thereof, or of any authority established by the general court to serve a public purpose, unless such materials or data fall within the following exemptions in that they are:

(1) specifically or by necessary implication exempted from disclosure by statute;
(2) related solely to internal personnel rules and practices of the government unit, provided however, that such records shall be withheld only to the extent that proper performance of necessary governmental functions requires such withholding;

(3) personnel and medical files or information; also any other materials or data relating to a specifically named individual, the disclosure of which may constitute an invasion of personal privacy;

(4) inter-agency or intra-agency memoranda or letters relating to policy positions being developed by the agency; but this subparagraph shall not apply to reasonably completed factua

(5) notebooks and other materials prepared by an employee of the commonwealth which are personal to him and not maintained as part of the files of the governmental unit;

(6) investigatory materials necessarily compiled out of the public view by law enforcement or other investigatory officials the disclosure of which materials would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest;

(7) trade secrets or commercial or financial information voluntarily provided to an agency for use in developing governmental policy and upon a promise of confidentiality; but this subparagraph shall not apply to information submitted as require by law or as a condition of receiving a governmental contract or other benefit;

(8) proposals and bids to enter into any contract or agreement until the time for the opening of bids in the case of proposals or bids to be opened publicly, and until the time for the receipt of bids or proposals has expired in all other cases;

(9) appraisals of real property to be acquired until (1) an agreement is entered into; or (2) three years have elapsed since the making of the appraisal; or until any litigation relative to such appraisal has been terminated, whichever occurs first.
(q) "University"

"University" shall mean the University as a whole, including all of its campuses and constituent elements.

Part II - Administration

§201 Identification and maintenance

Each campus shall identify the kinds of personal data held, and shall maintain such data with such accuracy, completeness, timeliness, pertinence and relevance as is necessary to assure fair determination of a data subject's qualifications, character, rights, opportunities or benefits when such determinations are based upon such data.

§202 Individual in charge of personal data system

Each campus shall, for each personal data system it maintains, designate one person who serves as the officer immediately responsible for such system.

§203 Additional procedures

Each campus may, subject to the approval of the Board, adopt such supplemental procedures not inconsistent with these regulations as may be deemed necessary or convenient to the accomplishment of the purposes of G.L. c. 66A.

§204 Holder agreements

Any campus 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 these regulations, shall contain provisions requiring compliance with the regulations. Where agreements are absent, agencies shall arrange for the development of the same in order to require compliance with these regulations.
§205 Personnel Security

Each campus shall permit only those employees whose duties require it to have access to personal data, and shall:

(a) keep to a minimum the number of employees whose duties involve access to personal data;

(b) inform existing personnel concerning standards of confidentiality and security required by these regulations;

(c) not allow any other agency or individual not employed by the University to have access to personal data unless such access is authorized by statute or regulation, or is approved by the campus and by the data subject whose personal data are held, or is required in order to comply with a judicial order or pursuant to any lawfully issued subpoena, provided, that the officer immediately in charge of the data, or his designee, shall make a reasonable effort to notify the data subject in advance of compliance therewith; or in a situation of emergency, if access to the data is necessary to protect the health or safety of the data subject or of other persons.

§206 Physical Security

Each campus shall take reasonable precautions to protect personal data from dangers of fire, theft, unauthorized access, flood, natural disaster or other physical threat.

§207 Periodic review of data held; expunction of obsolete data

Each campus shall periodically, or at the request of the data subject, review its personal data systems with respect to the accuracy, current need, relevance and timeliness of data held. The campus shall expunge all obsolete personal data in accordance with existing University policy on the keeping of records. If any data subject desires some item which he deems inappropriate removed from his file or amended, the provisions of §§313-317 shall apply.

§208 Use of personal data for unrelated purposes

Except where otherwise provided by statute, regulation or judicial order, personal data collected for one or more purposes, shall not be used for another unrelated purpose without informing the data subject and receiving his approval.
§209 Duplicate Files

(a) Each holder shall insure that the number of duplicate files of personal data is maintained at an absolute minimum.

(b) Each holder shall insure that any duplicate file systems are maintained consistent with the requirements of these regulations.

§210 Audit Trail

Each holder shall maintain the most feasibly precise records indicating the names of all persons who have requested or gained access to personal data on a data subject, and the interest such person has expressed in obtaining such access. Such records or audit trails shall conform to the following requirements:

(a) where such data are held in computerized form, the data system shall have the capacity for a program or programs to record electronically all persons having access to and uses of personal data;

(b) where the data are held in manual form, the holder shall require that a manual notation be made, to the maximum extent possible, of all persons having access to and uses of the data;

(c) where the duties of University personnel require frequent or routine access to personal data, the fact of each such use of data need not be listed, but the fact that such personnel have routine access shall be published in an appropriate manner.

(d) the audit trail record shall be treated as personal data under these regulations for purposes of determining who shall have access to such audit trail.

§211 Dissemination - notice to subsequent holders

Each holder, when disseminating personal data, shall ensure that any subsequent holder is aware of the requirements of these regulations, G.L. c. 66A, other pertinent statutes, and any written policy directive developed by such campus 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.
(a) identification and justification of personal data as essential in accordance with Part 300;

(b) brief descriptions of existing or planned agreements involving the holding of personal data in accordance with section 300.5;

(c) 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 sections 301.6 and 301.8 herein; and

(d) 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 these regulations.

§212 Automation of Personal Data

Each campus, 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:

(a) assure that such automation will be in compliance with each of the mandates presented in this part, particularly, provisions for an annual report, an audit trail and for periodic review of data held, in accordance with §§207,210 and 213 herein; and

(b) 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 these regulations.

§213 Notice and annual report to the Secretary of State and the Board

Each campus shall be September 1, 1976, and annually thereafter, and upon the subsequent establishment, termination, or change in character of a personal data system file a report with the Secretary of State and the Board regarding each personal data system it operates. 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 campus 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 G.L. c. 66A and

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

§214 Directory Information

Directory information, as defined in §103(f) above, may be disseminated generally, provided, that each campus shall cause to be published a statement listing the types of directory information it intends to publish or disseminate, and shall provide an opportunity for data subjects to request that such information concerning them not be published or disseminated except as required for University purposes.

Part III - Rights of Data Subjects

§301 Holding - Notice to data subjects

Each campus shall inform data subjects of their rights under these regulations and other pertinent statutes of the type of data held by the agency, the length of time of such holding, and the expected uses of such data. Such notice may be given by posting general descriptions of data systems in appropriate places or by publication. No personal identifier shall be used in such posting or publication.

§302 Requests on data

A holder, upon request of an individual, shall inform the individual, in writing, whether such holder maintains any personal data concerning him.

§303 Statement of rights

A holder shall furnish to any person requested to provide personal data a statement listing all individual rights set forth in these regulations.
§304 Right of access of data subject

Each data subject shall, upon written request, have access to any personal data concerning him, except where prohibited by law or judicial order or where the subject has waived his right to have such access pursuant to §308. Such personal data shall be made available to the subject in a form comprehensible to him, and if failure to provide the subject with a copy of the data would effectively prevent him from exercising his right to inspect and review his records, a copy of such data shall be provided to said subject upon payment of a reasonable charge not to exceed the actual cost of producing such copy. If the records of any data subject include personal data concerning any other individual, said data subject shall have the right to inspect and review only such portion of said records as relates solely to the data subject.

§305 Rules governing access to data

A holder may adopt reasonable written rules governing access to personal data, consistent with these regulations and all pertinent legislation, which:

(a) insure 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; provided that the time for inspection shall not be unduly restricted nor shall an unreasonable cost for copying be charged; and

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

§306 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 data, only if the denial of access is permitted by statute.

§307 Notification of denial of access to data

A holder shall notify in writing any individual of its denial of his request for access, the reasons therefore, and the rights of appeal set forth in §§315-317.

§308 Waiver of right of access to certain data

A data subject may waive his right of access to confidential letters or statements of recommendation or evaluation, provided (a) that §310 of these regulations shall have been complied with; (b) that the data subject, upon request, shall have been informed of the names of all persons submitting confidential recommendations or evaluations; (c) that such recommendations or evaluations shall be used solely for the purpose for which they were specifically intended; (d) that no data
subject shall be required to waive his right of access; and (e) that if such data subject shall have declined to waive his right of access, any person requested to submit a recommendation shall be so informed.

§309 Right to give or to withhold informed consent or waiver

Each data subject may give or withhold informed consent or waiver when requested by any holder to provide personal data.

§310 Criteria for informed consent or waiver

(a) Consent or waiver may be deemed to be "informed" only if the holder provides the following information to the data subject and the data subject indicates his understanding and agreement:

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

(ii) 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;

(iii) 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 ; and

(iv) 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.

§311 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.
§312 Duties of information officers

Each officer described in §202 shall ensure that all data subjects enjoy the rights provided under these regulations, and under G.L. c. 66A, and he shall—

(a) receive complaints and objections;
(b) answer questions; and
(c) direct operations—

with respect to the privacy, confidentiality, and security of personal data.

§313 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 officer in immediate charge of the personal data system complained against. Should said officer be unavailable, the data subject may make his objection to the next immediate superior of such officer who is available.

§314 Responsibilities of holder pursuant to objection

Pursuant to an objection by a data subject, the officer in immediate charge of data systems shall within thirty (30) days of the receipt of the objection:

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

(b) investigate the validity of the objection; and

(c) if, after the investigation—

(i) 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,

(ii) 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;

—-and
(d) notify, in writing, the appropriate individual under whose authority personal data is held regarding the action taken.

§315 Appeal of officer'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 campus head under whose authority the personal data in question are held. Such appeal shall be filed in writing within thirty (30) days of notification of the decision by the officer in charge of the personal data system.

§316 Campus head; adjudicatory hearing

A campus head or his designee hearing an appeal filed pursuant to section 315 shall—

(a) at the behest of the appellant data subject conduct a hearing within thirty (30) days of the receipt of such appeal, and render a decision on the merits within thirty (30) days of the conclusion of said hearing;

(b) notify, within seven (7) days of rendering of a decision, in writing, the appellant data subject and the appellee holder regarding the nature of the decision.

§317 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 complained of.

§318 Judicial relief

No provision of this Part 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 G.L. c. 214, §3B, as added by St. 1975, c. 776, §3.
Part IV - Enforcement

(a) Employees of the University of Massachusetts:

Any employee of the University 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 President or Chancellor consistent with the rules and regulations of the Board and laws of the Commonwealth governing its employees, and may be denied future access to personal data and removed from any holding responsibilities. In addition to the remedies provided in G.L. c. 214, §3B, as added by St. 1975, c. 776, §3, the President or Chancellor may by administrative action revoke the authorization to hold personal data of any officer, employee, college, school, department, agency, institute or station under his supervision.

(b) Non-University holders:

Any holder, other than a campus defined under §103(c), found breaching the confidentiality of data subjects through violation of these regulations shall be subject to a review and an investigation of the President or Chancellor which may lead to suspension of any contractual or licensure relationship and to legal sanctions brought by the Attorney General.

§402 Monitoring of compliance

(a) Each campus head shall be responsible for monitoring compliance with these regulations with respect to each personal data system under his general supervision.

(b) The board, or its designee, pursuant to G.L. c. 66A, §3, shall exercise its approval authority with regard to supplemental procedures promulgated by the various campuses.