MODEL MASSACHUSETTS PRIVACY LEGISLATION[1]

1. LIMITATIONS ON ACCESS TO, OR DISCLOSURE OF, PERSONALLY IDENTIFIABLE INFORMATION.

(A) AUTHORIZED REPRESENTATIVES.[2] The Department of Elementary and Secondary Education (DESE) and District Boards of Education shall only designate parties that are under their direct control to act as their authorized representatives to conduct any audit or evaluation, or any compliance or enforcement activity in connection with legal requirements that relate to state or district supported educational programs, when any such audit, evaluation or activity requires or is used as the basis for granting access to personally identifiable student information;

(B) OUTSOURCING.[3] DESE, District Boards of Education and institutions may not disclose personally identifiable information from education records of students without the written consent of eligible students or parents to a contractor, consultant, or other party to whom an agency or institution has outsourced institutional services or functions unless that outside party:

(1) performs an institutional service or function for which DESE, District Board of Education, or institution would otherwise use employees;[4]

[1] Adapted from model legislation by Leonie Haimson of Class Size Matters and Barmak Nassirian

[2] FERPA has historically allowed non-consensual access to education records to "authorized representatives" of the Comptroller General of the United States, the Secretary, the Attorney General, and to state and local educational authorities for certain legislatively specified purposes. The 2011 FERPA Final Regulations opened a huge loophole in FERPA by explicitly allowing the officials listed above to designate other entities as their "authorized representative," even if such entities were not under their direct control. Educational authorities can, under the post 2011 regs, designate the state department of labor, or the chief of police, or the head of the bureau of prisons as their authorized representative and thus enable them to access to education records without prior consent. Subsection (A) plugs this loophole and restores the pre-2011 settled law by limiting the ability of the state and local educational authorities to designate entities that they don't control as their authorized representatives.

[3] State and local education agencies routinely contract with third-parties for services that may involve disclosure of personally identifiable information from education records. The 2008 FERPA regulations, for the first time, explicitly permitted this, but failed to adequately address privacy and security issues. Subsection (B) articulates specific requirements that contractors must meet in order to qualify for non-consensual access to education records.

[4] Attempts to limit the scope in order to prevent gaming. The function must be sufficiently necessary that the institution, district or state would otherwise carry it out using employees.

(2) is under the direct control[5] of the agency or institution with respect to the use and maintenance of education records;
(3) limits internal access to education records to those individuals that are determined to have legitimate educational interests;[6]
(4) does not use the education records for any other purposes[7] than those explicitly authorized in its contract;
(5) does not disclose any personally identifiable information to any other party:[8]

(I) without the prior written consent of the parent or eligible student, or
(II) unless required by statute or court order and the party provides a notice of the disclosure to DESE, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

(6) maintains reasonable administrative, technical and physical safeguards[9] to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
(7) uses encryption technologies[10] to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5;
(8) has sufficient administrative and technical procedures to monitor continuously[11] the security of personally identifiable information in its custody;
(9) conducts a security audit annually and provides the results[12] of that audit to each Department, District Board of Education, or institution that provided educational records;

---

[5] Ensures that third-party recipients are subject to direct control with regard to any personally identifiable information they receive.

[6] Further limits access *within* the receiving organization by imposing the same condition that FERPA applies to principals.

[7] Prohibits repurposing of personally identifiable information by contractors.

[8] Prevents non-consensual re-disclosures, unless legally required, and prevents mission creep and cascading re-disclosures that can quickly fall way outside justifications originally offered for the initial disclosure.

[9] Mandates reasonable qualifications that all contractor must meet in order to qualify.

[10] Almost all contractors use or claim to use some type of encryption, but rarely disclose exactly how robust their encryption technology is. This references HHS encryption standards for medical records, which are almost invariably co-mingled with education records at most institutions.

[11] Requires constant monitoring, not just an annual review.

[12] Mandates annual audit that **must** be provided to contracting party.

(10) provides DESE, District Board of Education, or institution with a breach remediation plan[13] acceptable to DESE, District Board of Education or institution prior to initial receipt of education records;
(11) reports all suspected security breaches to DESE, District Boards of Education, or institution that provided education records as soon as possible but not later than forty-eight hours after a suspected breach was known or would have been known by exercising reasonable diligence;[14]
(12) reports all actual security breaches to DESE, District Boards of Education, or institution that provided education records as soon as possible but not later than twenty-four hours[15] after an actual breach was known or would have been known by exercising reasonable diligence;
(13) in the event of a security breach or unauthorized disclosures of personally identifiable information, pays all costs and liabilities[16] incurred by DESE, District Boards of Education, or institutions related to the security breach or unauthorized disclosure, including but not limited to the costs of responding to inquiries about the security breach or unauthorized disclosure, of notifying subjects of personally identifiable information about the breach, of mitigating the effects of the breach for the subjects of personally identifiable information, and of investigating the cause or consequences of the security breach or unauthorized disclosure; and
(14) destroys or returns[17] to DESE, District Boards of Education, or institutions all personally identifiable information in its custody upon request and at the termination of the contract.

(C) STUDIES.[18] DESE, District Boards of Education, or institutions may disclose personally identifiable information from an education record of a student without the consent of eligible students or parents to a party conducting studies for, or on behalf of, educational agencies or institutions to:

(1) develop, validate, or administer predictive tests;

---

[13] They have to have a plan in advance, not just make it up after a breach.

[14] Many contracts only require notification if the contractor decides—at its sole discretion—that a breach has in fact occurred. This requires contractors to report suspected breaches.

[15] Actual breaches are subject to a tighter reporting timeline. Note that the use of "reasonable diligence" comes from HIPAA breach notification rule.

[16] Financial indemnification.

[17] Explicit record retention rule.

[18] The 2011 FERPA regs created a loophole to allow non-consensual disclosure and subsequent re-disclosures of personally identifiable information to entities purporting to be conducting studies for or on behalf of institutions. This language ensures that third-parties seeking non-consensual access to personally identifiable information from education records meet the same reasonable conditions set forth for contractors.

(2) administer student aid programs; or
(3) improve instruction;
provided that the outside party conducting the study meets all of the requirements for contractors set forth in paragraph (B) of this subdivision;

(D) PUBLIC DISCLOSURES.[19] Prior to any non-consensual disclosures authorized by paragraphs (B) and (C) of this section, DESE, District Boards of Education, and institutions shall publicly and conspicuously disclose on their web sites and through electronic notification to the chairs of the assembly and senate education committees the existence and character of any contracts or agreements pursuant to which they intend to disclose personally identifiable information from education records to a contractor, outsourcing entity, or third party conducting a study. Such disclosure and notification shall include:

(1) the name and location of the data repository where any personally identifiable information would be maintained by a contractor, outsourcing entity or third party;
(2) the principal purpose or purposes for which the information is intended to be used;
(3) the categories of individuals whose records would be disclosed to the contractor, outsourcing entity, or third party;
(4) the categories of records maintained by the contractor, outsourcing entity, or third party;
(5) expected uses of the records disclosed to the contractor, outsourcing entity, or third party;
(6) the policies and practices of the contractor, outsourcing entity, or third party regarding storage, retrievability, access controls, retention, and disposal of the records;
(7) the title and business address of DESE, District Board of Education, or institutional official who is responsible for the contract or agreement, and the name and business address of the contractor, outsourcing entity, or third party directly responsible for education records maintained pursuant to said contract or agreement;
(8) the procedures whereby eligible students or parents can be notified at their request how to gain access to any record pertaining to them or their children maintained by the contractor, outsourcing entity, or third party, and how they can contest its content; and
(9) the categories of sources of records in the data repository containing education records;

(E) COMMERCIAL USE PROHIBITED.[20] DESE, District Boards of Education and institutions may not, without the written consent of eligible students or parents, facilitate, arrange, contract for

[19] This section articulates the specific disclosures that must be made to parents before schools, districts, or the state can share personally identifiable information with contractors/researchers without their consent, as allowed under (B) & (C). Intent is to allow for pragmatic, reasonable use of contractors but prevent sloppy privacy/security practices by ensuring reasonable transparency. If schools can't answer these basic questions, they haven't thought the contract through.

[20] Prevents development of commercial products or services without parental consent.

or authorize a third-party to collect personally identifiable information of its students,[21] or disclose personally identifiable information from education records to any party for a commercial use, including but not limited to marketing products or services, compilation of lists for sale or rental, development of products or services, or creation of individual, household, or group profiles; nor may such disclosure be made for provision of services other than contracting, studies, and audits or evaluations as authorized and limited by paragraphs (B) and (C) of this subdivision. Any consent from an eligible student or parent must be signed by the student or parent, be dated on the day it was signed, not have been signed more than six months prior to the disclosure, must identify the recipient and the purpose of the disclosure, and must state that the information will only be used for that purpose and will not be used or disclosed for any other purpose.

2. DATA REPOSITORIES AND INFORMATION PRACTICES.[22]

(A) DESE and District Boards of Education may not, directly or through contracts with outside parties, maintain personally identifiable information from education records without the written consent of eligible students or parents unless maintenance of such information is:

(1) explicitly mandated in federal or state statute;[23]

(2) administratively required for the proper performance of their duties under the law and is relevant to and necessary for delivery of services;[24] or

(3) designed to support a study of students or former students, provided that no personally identifiable information is retained on former students longer than five years after the date of their last enrollment at an institution.[25]

(B) DESE and District Boards of Education shall publicly and conspicuously disclose on their web sites and through annual electronic notification to the chairs of the assembly and senate education committees[26] the existence and character of any personally identifiable information from education records that they, directly or through contracts with outside parties, maintain. Such disclosure and notifications shall include:[27]

---

[21] Addresses COPPA-FERPA gap.

[22] Addresses privacy practices of longitudinal data repositories and state-sanctioned data marts. Modeled after federal Privacy Act of 1974, with minor modifications to align the language with FERPA.

[23] Ensures public disclosure of every data element.

[24] Ensures intentionality and minimizes the collection and retention on unnecessary data.

[25] Ensures against permanent collection of data in the name of longitudinal studies.

[26] This could be altered to require notice to the public.

[27] These are just fair information practices that would force the states and districts to think really hard before creating massive data systems that become the targets of authorized and unauthorized snooping.

(1) the name and location of the data repository where such information is maintained;
(2) the legal authority which authorizes the establishment and existence of the data repository;
(3) the principal purpose or purposes for which the information is intended to be used;
(4) the categories of individuals on whom records are maintained in the data repository;
(5) the categories of records maintained in the data repository;
(6) each expected disclosure of the records contained in the data repository, including the categories of recipients and the purpose of such disclosure;
(7) the policies and practices of DESE or the District Boards of Education regarding storage, retrievability, access controls, retention, and disposal of the records;
(8) the title and business address of DESE or District Board of Education official who is responsible for the data repository, and the name and business address of any contractor or other outside party maintaining the data repository for or on behalf of DESE or the District Board of Education;
(9) the procedures whereby eligible students or parents can be notified at their request if the data repository contains a record pertaining to them or their children;
(10) the procedures whereby eligible students or parents can be notified at their request how to gain access to any record pertaining to them or their children contained in the data repository, and how they can contest its content; and
(11) the categories of sources of records in the data repository;

(C) DESE, District Boards of Education, and institutions may not append education records with personally identifiable information obtained from other federal or state agencies through data matches[28] without the written consent of eligible students or parents unless such data matches are:

(1) explicitly mandated in federal or state statute; or
(2) administratively required for the proper performance of their duties under the law and are relevant to and necessary for delivery of services.

3. **PENALTIES AND ENFORCEMENT.**
(A) Each violation of any provision of this section by an organization or entity that is not DESE, a District Board of Education, or an institution as defined in paragraph (B) of subdivision one of this section shall be punishable by a civil penalty of up to one thousand dollars; a second violation by the same organization or entity involving the educational records and privacy of the same student shall be punishable by a civil penalty of up to five thousand dollars; any subsequent violation by the same organization or entity involving the educational records and privacy of the same student shall be punishable by a civil penalty of up to ten thousand dollars; and each violation involving a different individual educational record or a different individual student shall be considered a separate violation for purposes of civil penalties;

[28] This provision would prevent data-mining through linkages with non-educational data sources, and would prohibit concatenation of data from multiple sources (for example juvenile justice, military, unemployment insurance, etc.).

(B) The attorney general shall have the authority to enforce compliance with this section by investigation and subsequent commencement of a civil action, to seek civil penalties for violations of this section, and to seek appropriate injunctive relief, including but not limited to a prohibition on obtaining personally identifiable information for an appropriate time period. In carrying out such investigation and in maintaining such civil action the attorney general or any deputy or assistant attorney general is authorized to subpoena witnesses, compel their attendance, examine them under oath and require that any books, records, documents, papers, or electronic records relevant or material to the inquiry be turned over for inspection, examination or audit, pursuant to the civil practice law and rules; subpoenas issued pursuant to this paragraph may be enforced pursuant to the civil practice law and rules.
(C) Nothing contained herein shall be construed as creating a private right of action against DESE, a District Board of Education, or an institution as defined in paragraph (B) of subdivision one of this section.

4. **ADMINISTRATIVE USE.** Nothing in this section shall limit the administrative use of education records by a person acting exclusively in the person's capacity as an employee of a school, a District Board of Education or of the state or any of its political subdivisions, any court or the federal government that is otherwise required by law.