Federal and State Laws Governing Access to Student Data

FERPA, PPRA, COPPA

Minnesota Government Data Practices Act

FERPA Overview

Family Educational Rights and Privacy Act (FERPA/1974) makes education data in student records private and generally allows parents to control access to their students' data

Regulations appear in: 20 U.S.C. 1232g ; 34 C.F.R. § 99

FERPA Applies to Education Agencies and Institutions

FERPA applies to public and private schools, school districts, state education agencies, and other education institutions that (1) receive federal US DOE funds, and (2) provide educational services or instruction or direct or control an education institution

34 C.F.R. §§ 99.1(a), 99.1(c)(1), 99.1(c)(2)

FERPA Protects the Confidentiality of Education Records

"Education records" are (1) materials such as records and files maintained by an education agency or institution or by a teacher, administrator, or other school employee from that agency or institution, and (2) that contain information directly related to a student

20 U.S.C. § 1232g(a)(4)A; see Owasso Independent School District v. Falvo, 534 U.S. 426, 433-34 (2002)

Parents and Eligible Students Have Rights Under FERPA

- FERPA gives parents rights to protect and access their children's education records
- These rights transfer to students when they reach age 18 or attend postsecondary institutions

20 U.S.C. §§ 1232g(a)(1)(A), 1232g(a)(1)(D)(2), 1232g(b)(2) (2006)

Parents Must Consent to Disclosing a Student's PII

Education institutions must obtain a parent's written consent before disclosing Personally Identifiable Information (PII) in a student's record, unless an exception applies

34 C.F.R. §§ 99.30(a) and 99.31

Schools Must Tell Parents About Their Rights to Inspect and Review Records

Schools annually must tell parents and eligible students about their rights to inspect, review, and amend students' records, consent to disclosing PII, and file a noncompliance complaint

34 C.F.R. §§ 99.7(a)(2)(i), 99.7(a)(2)(ii), 99.7(a)(2)(iii), 99.7(a)(1)(iv)

Schools Must Record Requests for PII

Schools must record each request for and each disclosure of PII in a student's education record unless the disclosure is to a parent, school official, or person with written consent from the parent, or the information is obtained through a subpoena or other court order

34 C.F.R. §§ 99.32(a)(1), 99.32(d)

Schools May Disclose Student Directory Information, De-identified Information, and Some PII Without Consent

Schools May Disclose Directory Information Without Consent

- Schools may disclose directory information to anyone without consent
- Schools decide what information to designate as directory information
- Schools must notify parents about disclosing directory information and allow parents to refuse to disclose the information

20 U.S.C. § 1232(g)(a)(5)(B) (2006)

Schools May Disclose De-identified Information Without Consent

- De-identified data require a school to remove all PII and to determine that a student is not personally identifiable
- Schools may disclose de-identified data for research purposes

34 C.F.R. § 99.31(1b)(b)(1)

Schools May Disclose PII Without Consent if an Exception Applies:

Schools may disclose PII without consent to:

- School officials with "legitimate educational interests"
  - Cloud computing service providers may be considered school officials
  - Cloud computing service providers may be subject to the Federal Trade Commission and the Children's Online Privacy Protection Act

34 C.F.R. §§ 99.31(a), 99.31(a)(1)(i)(A); 20 U.S.C. § 1232g(b)(1)(A) (2006)

Schools May Disclose PII Without Consent if an Exception Applies:

- A contractor, consultant, or other entity to which school officials outsource institutional services under some circumstances

34 C.F.R. §99.31(a)(1)(i)(B)

Schools May Disclose PII Without Consent if an Exception Applies:

- Schools may disclose PII to officials performing certain functions
- State and local authorities within the juvenile justice system
- Accrediting organizations

34 C.F.R. §§ 99.31(a)(2), 99.34(a), 99.31(a)(3), 99.31(a)(4), 99.31(a)(b)(i), 99.31(13)-(16), 99.36(a); 20 U.S.C. §§ 1232g(a)(5)(E), 1232g(a)(5)(G) (2006)

Protection of Pupil Rights Amendment (PPRA) Applies to K-12 Schools

- Protects uses of students' PII collected for marketing purposes or surveys and evaluations
- Allows parents to inspect survey materials and requires parent consent if surveys reveal certain information about the student or the student's family

20 U.S.C. § 1232h; 34 C.F.R. § 98

Children's Online Privacy Protection Act (COPPA)

COPPA establishes privacy standards and obligations for commercial website operators and online service providers collecting personal information from children under 13

15 U.S.C. §§ 6501-6506 (1998); 16 C.F.R. § 312 (2013)

Government Data Practices Act Regulates Data Practices in Minnesota

- FERPA sets minimum data practices standards that states may supplement
- Minnesota Government Data Practices Act in Minnesota Statutes, chapter 13, regulates government data practices
- Minnesota law adopts FERPA and adds other restrictions and requirements

The Minnesota Government Data Practices Act Differs From FERPA by:

- Requiring a Tennessen warning
  Minn. Stat. § 13.04, subd. 2
- Allowing a minor student to give informed consent to disclose educational data
  Minn. Stat. § 13.02, subd. 8
- Allowing a minor student to request that a school deny the student's parents access to data about the student
  Minn. Stat. § 13.02, subd. 8

The Minnesota Government Data Practices Act Differs From FERPA by:

- Releasing education records subject to a court order but not a subpoena
  Minn. Stat. § 13.32, subd. 3(b)
- Prohibiting parents from inspecting teachers' desk notes but allowing parents to inspect the desk notes of other school personnel
  Minn. Stat. § 13.32, subd. 1(a)
- Allowing parents to designate an additional person to participate in school conferences
  Minn. Stat. § 13.32, subd. 10a

States' Laws on Student Data Use, Privacy, and Security

New state laws fall into one of three areas:

- Prohibiting entities from collecting certain categories of student data
- Improving state and local data governance policies and practices
- Establishing guidelines for how third parties handle student data

Minnesota Collects Lots of Student Accountability Data

Testing Data

- No Child Left Behind Act
  20 U.S.C. §§ 6301-7916 (2002)
  - Title I, Part A
  - Title I, Part C
  - Title I, Part D
- Annual school performance reports
  Minn. Stat. § 120B.36

Minnesota Students' Education and Workforce Data

- Minnesota's State Longitudinal Educational Data System (SLEDS) has lots of pre-K through college and career data on students
  Minn. Stat. § 127A.70, subd. 2(b)
- SLEDS has a four-part framework to help answer policy makers' questions about program effectiveness and target improvement strategies:
  - Pathways
  - Progress
  - Predictors
  - Performance

Minnesota Student Survey Data

- Minnesota Student Survey (MSS) is a partnership between Minnesota Departments of Education, Health, Human Services, and Public Safety
- MMS asks young people about their activities, opinions, behaviors, and experiences
- MMS provides data for program planning and evaluation
  - Student participation is voluntary; surveys are anonymous

Examples of Issues Related to Student Data Use, Privacy, and Security

(1) Privacy Protections for Longitudinal Databases

- Many states, districts, and schools collect student information beyond what's needed under the No Child Left Behind Act
- Longitudinal databases hold directory, demographic, disciplinary, academic, health, and family information about each child and may hold information about pregnancies, mental health, illness, jail sentences, family wealth indicators

(1) Privacy Protections for Longitudinal Databases

- Anonymized state level data
- Comprehensive third party agreements
- Limits on collecting information
- Data retention policies
- Access and permissible use policies
- Audit logs
- Publicly available information

(1) Privacy Protections for Longitudinal Databases

- Important to know who has access, purposes for access, de-identifying policies, FERPA and Minnesota law
- Minnesota has no explicit privacy protections for longitudinal databases

(2) School Data Storage and Retention Policies

- Schools collect lots of student data
- Creating and implementing secure student data management policies and practices may be difficult

(3) Third Party Contracts

- FERPA allows schools to share directory information with third parties
- Few parents opt out
- Many school districts use online service providers for scheduling, data processing/managing
- District agreements may or may not restrict vendors' use of student information or the sale or marketing of the information

(4) Access, Use, and Security of State Databases

- Comprehensive state databases raise concerns about access, security, and how student data will be used
- Minnesota's SLEDS governing board is working on policies for permissible data use, access, and security

(5) Vendors' Use of Student Data Not in Students' Education Records

- Third party vendors may collect and combine the student data with other personal data from nonschool sources sufficient to develop student profiles and target advertising to students
- Vendors may sell or exchange student profiles

(6) Students' Ability to Delete Their Digital Footprint

- Family, friends, college admissions officers, and potential employers can see students' digital footprint
- California enacted an "eraser button" law effective 2015

(7) Students' Ability to Limit the Use of Their Personal Information

California's new student data privacy law prohibits K-12 websites, online services, and apps from using, selling, or disclosing students' online searches, text messages, photos, voice recordings, biometric data, location information, food purchases, political or religious information, digital documents, or student ID codes

(8) Vendors' Ability to Market Products, Apps, Materials, and Games

- Minnesota law does not prevent third party school vendors from marketing to students
- California's new student data privacy law explicitly prohibits third parties from targeting and marketing to students

(9) Inconsistent and Subjective Student Discipline Reports

Students are disciplined for “willful defiance” or “disruption” or “disorderly conduct” – terms without a clear or standard definition

- Student records may be unreliable, harmful, and exacerbate racial disparities

Foundation for a State Education Data Privacy and Security Policy

- Acknowledge the value of education data and the importance of protecting the data
- Direct an entity to oversee privacy and security policies and practices
- Create a data inventory and describe data collected and the purpose for the data
- Promote public transparency
- Establish statewide protections for PII
- Require a data security plan