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) protects the privacy of students and parents.

- Right to inspect and review education records.
- Right to request amendment of education records.
- Restrictions on disclosure of information.

20 U.S.C. § 1232g ; 34 C.F.R. part 99

FERPA Applies to Education Agencies and Institutions

Education institutions that (1) receive federal US DOE funds, and (2) provide educational services or instruction or direct or control an education institution.

- Public and private schools
- School districts
- State education agencies

“Education Records”

Information recorded in any way that

(1) Contains information directly related to a student, and

(2) Is maintained by an education agency or institution or by a party acting for the agency or institution.

Parents and Eligible Students Have Rights Under FERPA

- Inspect and review education records.
  - Parents' rights transfer to students when they reach age 18 or attend postsecondary institutions ("eligible students").
- Request amendment of education records.
  - Formal hearing process.
  - Written comments about contested information in the records.
- Consent to disclosures, with some exceptions.
- File a complaint with US DOE. No private cause of action.

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.
- PII includes name, address, Social Security Number, mother's maiden name, etc.

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.

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;
- the party seeks directory information; or
- the information is obtained through a subpoena or other court order.

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.

Schools May Disclose De-identified Information Without Consent

- To disclose de-identified data, school must remove all PII and determine that a student is not personally identifiable.
- Schools may disclose de-identified data for research purposes.

Schools May Disclose PII Without Consent if an Exception Applies:

Schools may disclose PII without consent to:

- School officials with "legitimate educational interests;" contractors, consultants, volunteers performing institutional functions.
  - Cloud computing service providers may be subject to the Federal Trade Commission's Children's Online Privacy Protection Act.

Schools May Disclose PII Without Consent if an Exception Applies:

- Officials of another school where the student seeks to enroll.
- Certain other governmental entities or officials.
- In connection with financial aid the student has applied for or received.
- Testing purposes.

Schools May Disclose PII Without Consent if an Exception Applies:

- Accrediting organizations.
- State and local authorities within the juvenile justice system.
- Subpoena.
- Health or safety emergency.

Students With Disabilities

- FERPA and Individuals with Disabilities Education Act (IDEA) together govern access to education records of students with disabilities.
- IDEA governs access to records related to student's disability and education services provided under an individual education plan.
- IDEA has additional crime reporting provisions that work with FERPA.

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

COPPA

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

The Children's Online Privacy Protection Act (COPPA 1998) requires the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The amended rules took effect on July 1, 2013. The rules require that operators, which are commercial websites and online services, must:

- Post a clear and comprehensive online privacy policy describing their information practices for personal information collected online from children
- Provide direct notice to parents and obtain verifiable parental consent

Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

COPPA – cont.

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

- Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties
- Provide parents access to their child's personal information to review and/or have the information deleted, and have the opportunity to prevent further use or online collection of a child's personal information
- Maintain the confidentiality, security, and integrity of information they collect from children and retain personal information collected online from a child for only as long as is necessary to fulfill the purpose for which it was collected

Federal Trade Commission, "Complying with COPPA: Frequently Asked Questions" https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Other Laws Related to Student Conduct on the Internet

Internet Filters in schools and libraries

Passed in 2000, and upheld by the Supreme Court in 2003, **The Children's Internet Protection Act (CIPA)** is a federal law that requires K-12 schools and libraries that receive federal funding to filter Internet content accessed by children.

Obscene Content

Minn. Stat. § 609.352 makes it a crime to solicit sexual content from a minor or to send sexual content to a minor

Cyberbullying

Minn. Stat. § 121A.031 prevents bullying via the Internet and social media

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

MDE Collects Student Data

- Federal mandates, e.g., ESEA, IDEA
- State mandates
  - Disciplinary data
  - Annual school performance reports
  - SLEDS
- Types of data
  - Testing
  - Enrollment
  - College readiness
  - Early learning

State Longitudinal Educational Data System (SLEDS)

- Matches student data from pre-K through completion of postsecondary education and into the workforce.
- Minnesota P-20 Partnership
  - expand reporting on outcomes, evaluate effectiveness of educational and workforce programs
  - evaluate the relationship between education and workforce outcomes. Minn. Stat. § 127A.20, subd. 2.
- Early Childhood Longitudinal Data Systems
  - data on growth and achievement in relation to participation in various state programs.

Minnesota Student Survey (MSS) Data

- Partnership between Minnesota Departments of Education, Health, Human Services, and Public Safety.
- Asks young people about their activities, opinions, behaviors, and experiences.
- Provides data for program planning and evaluation.
  - Student participation is voluntary; surveys are anonymous.

Issues Related to Student Data: Use, Privacy, and Security

Privacy Protections for Longitudinal Databases

Longitudinal Databases:

- What must be collected under state and federal law? What other data is collected?
- Is all the data aggregate data that is anonymous for any individual student?
- Do third parties agree to and follow privacy requirements?
- Should there be limits to what data is collected?
- What are the data retention policies?
- Are there access and use policies and audit logs on use?
- Is the information for the longitudinal studies available to the public?
- Aggregate data currently not covered by privacy statutes

School Data Storage and Retention Policies

There are concerns about how much data schools are collecting and maintaining:

- Use of school computers and tablets
- Use of software at school, on school provided electronic devices, and through home computers
- Many school districts use online service providers for scheduling, data processing/managing
- Internet and software allow students activities to be tracked, recorded, and saved

Third Party Contracts and Vendors

- FERPA allows schools to share directory information with third parties, and few parents opt out
- District agreements may or may not restrict vendors' use of student information or the sale or marketing of the information and vendors may sell or exchange student profiles
- 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

Third Party Contracts and Vendors – cont.

- Some states like California are trying to remedy these issues. California's 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, student IDs

- H.F. 1507 appears to be aimed at remedying the issues around third party contracts, and the technology schools use for record keeping and provide to students

Students' Ability to Delete Their Digital Footprint

- Outside school, what are student's privacy rights online?
- Family, friends, college admissions officers, and potential employers can see students' digital footprint
- California enacted the Privacy Rights for California Minors in the Digital World, an "eraser button" law, that became effective in 2015

House File 1507

Regulates the use, access, and distribution of data

- On electronic devices provided by the school
- On software used by students for school work and student records
- Broad definition for “educational data”

House File 1507

- The bill provides disclosures for parents and students about data

- The bill requires certain contract provisions to bind the schools and hardware and software providers. The contracts themselves, along with these new statutory provisions, FERPA, and the MDPA control what can be done with the data

- The bill creates additional rights and remedies for students and parents, as well as emergency provisions for accessing data in an emergency, and training requirements for schools