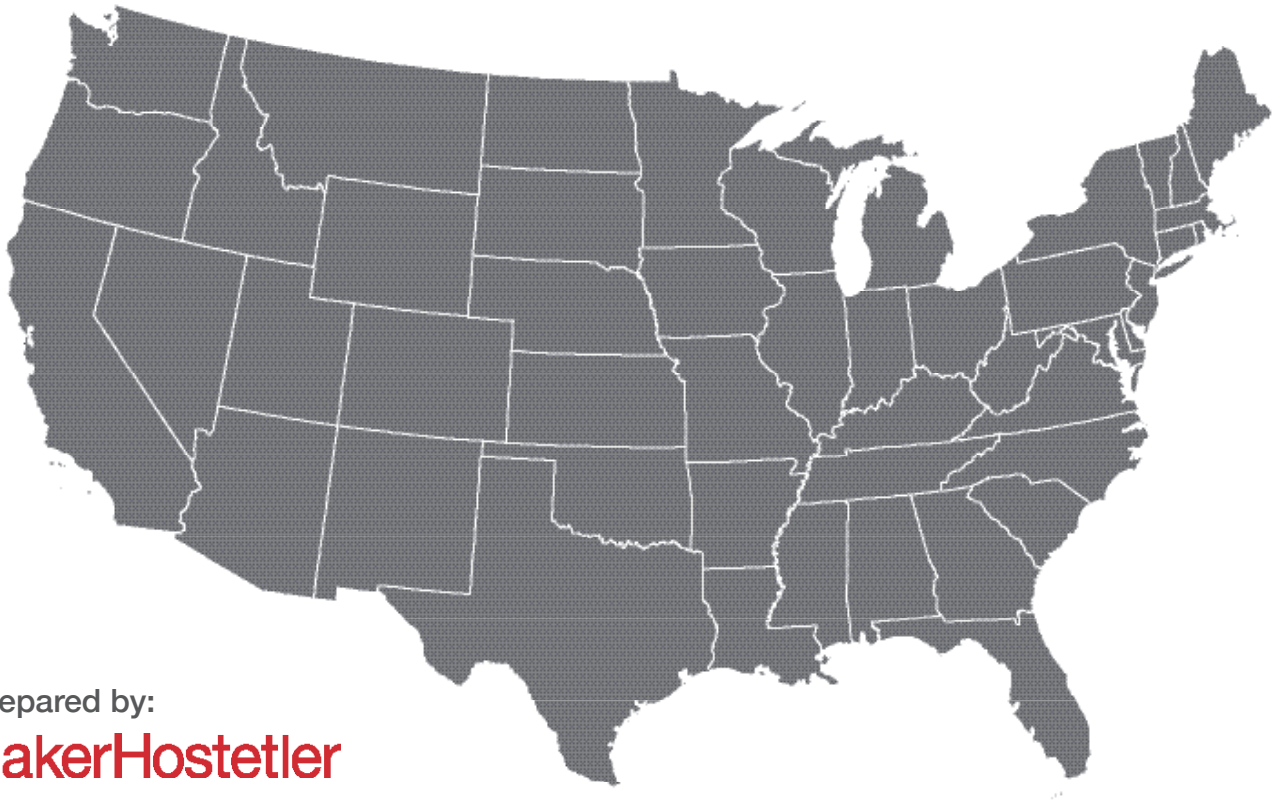
CENTER FOR DEMOCRACY & TECHNOLOGY

State Student Privacy Law Compendium

October 2016



Prepared by:

BakerHostetler

Table of Contents

This compendium is provided for informational purposes only. It does not constitute legal advice, and you should not rely on this information in lieu of obtaining such advice. You should consult legal counsel before any decisions or recommendations are made concerning the information contained in this compendium.

This compendium is a joint project between Center for Democracy & Technology (CDT) and BakerHostetler. Its preparation would not have been possible without the contribution of the following attorneys from BakerHostetler's data privacy team: Scott Koller, Jenna Felz, William Hellmuth, Kathryn Mellinger, Suchismita Pahi, and Paul Pittman.

Introduction

Student privacy has never faced greater challenges. While the practice of collecting data about students is not new – schools have been gathering and reporting test scores, grades, retention records, and the like for years – the means by which student data is collected, the types of data collected, and the entities that ultimately have access to this data have expanded dramatically. At the same time, stories of misuse of student data and poor data security practices have increased.

In response, state legislatures have proposed a number of laws to regulate student data collection, use, and sharing. For example, in 2015, state legislatures introduced over 180 bills, 28 of which were passed. CDT expects the number of student data privacy laws to increase exponentially over the next decade.

CDT has developed a state-by-state compendium of privacy laws relating to the collection, use, and sharing of student data. The compendium lists key student data privacy laws for all 50 states and the District of Columbia. The compendium is accurate as of October 2016. Please note that the compendium is neither intended to be and should not be used as a substitute for reviewing statutory language nor does it constitute legal advice. If you require more information please consult legal counsel.

Key Issue Areas for CDT's Compendium of State Student Privacy Laws

Definitions:

- How is "education record" defined (if at all)?
- What is considered "student data"?

Use Limitations:

- Does the law prohibit or limit sharing student data with third parties (such as advertisers)?
- If there are limitations on third party sharing, are there exceptions to these limitations (for researchers, product improvement, etc.)?

Data Minimization:

- Are there limits on how long data can be retained?
- Does the law require de-identification and/or aggregation in certain circumstances (i.e., when shared with researchers)?

Security:

- Does the law mandate specific security practices or the creation of a data security program?

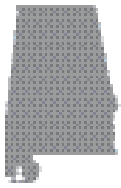
Auditing and Accountability:

- Must school districts and/or companies have a Chief Privacy Officer (CPO)?
- Is there a complaint process for students and/or parents when the state law has been violated?

Individual participation:

- Are parents and students able to opt-out of certain data collection or sharing?

Alabama



Applicable Laws

Title 16 of the Alabama Code governs Education

Provisions specifically related to privacy include: Ala. Educ. Code §§ 16-1-3 – 16-1-5; 16-1-41.1; 16-4-16; 16-5-7 16-5-32; 16-6B-7; 16-6C-2; 16-28-3.1; 16-44B-1

Definitions

"Educational Records"

There does not appear to be a general definition. However, with respect to children of members of the armed forces, Alabama defines "Education(al) Records" to mean "those official records, files, and data directly related to a student and maintained by the school or local education agency, including but not limited to records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs."

Ala. Educ. Code 16-44B-1

"Student Data"

Alabama defines "Student Unit Record" in the context of higher education, detailing those data elements that are to be included, at Ala. Educ. Code § 16-5-7.

Alabama further defines the data elements of a student record shall include, but not be limited to: (1) biographical and demographic data elements; (2) previous educational experience data elements; (3) current educational activity data elements; (4) residency status and whether the student pays tuition as a resident or a nonresident student. Ala. Educ. Code § 16-5-7 (b).

Use Limitations

Is sharing student data with third parties limited or prohibited?

Beyond provisions regarding sharing student data with the state educational authority (see e.g. Ala. Educ. Code §§ 16-1-41.1; 16-6C-2), Alabama does not appear to directly address sharing student data with third parties.

If so, are there exceptions?

N/A

Data Minimization

Are there data retention limits?

There is no specific retention limit noted in the statute; however, state and local educational authorities have the authority to destroy certain records that have been photographed or microphotographed. Further, the State Superintendent of Education "may prescribe the period for which records of certain classes [of records and other written materials] must be retained after having been photographed or microphotographed before such records are destroyed."

Ala. Educ. Code § 16-1-4.

Is de-identification or aggregation of data required?

Alabama does not appear to require de-identification or aggregation of data.

Security

Does the law mandate specific security practices or creation of a data security program?

Alabama does not appear to mandate a security program or specific security protocols.

Auditing and Accountability

Must school districts or companies have a CPO?

Alabama does not appear to require a CPO for school districts or companies.

Is there a complaint process when the law has been violated?

Alabama does not appear to have a prescribed complaint process for students or parents with respect to privacy violations or data breaches student data.

Individual Participation

Can parents/students opt-out of data collection or sharing?

Alabama does not appear to enable students and parents to opt-out of data collection or sharing.

Alaska

Applicable Laws

Title 14 of the Alaska Code governs "Education, Libraries, and Museums"

Including: Alaska Stat. §§ 14.34.010, 14.48.060

Title 4 of the Alaska Administrative Code governs "Education and Early Development"

Including: Alaska Admin. Code tit. 4 §§ 06.738, 06-895, 07.060, 19.099, 52.765, 59.005

Definitions

"Educational Records"

Under Alaska Admin. Code. tit. 4 § 07.060(a), "Each district shall maintain for each student a cumulative record consisting, at a minimum, of the following:

- subjects student has taken;
- grades earned and an explanation of the grading system used;
- units of credit earned;
- attendance records;
- scores student has recorded on standard tests taken;
- records of required immunizations and physical examinations and other health-related matters required by state law or district policy or bylaws; and
- beginning August 31, 2002, a unique 10-digit individual student identification number issued by the department."

Alaska outlines special requirements for educational records of military children (Alaska Stat. § 14.34.010) and postsecondary students (Alaska Stat. § 14.48.060) that are not addressed in this compendium.

"Student Data"

Alaska does not appear to define student data beyond "student learning data" (Alaska Admin. Code tit. 4 § 19.099(7)) that is limited to information on the student's performance.

Use Limitations

Is sharing student data with third parties limited or prohibited?

Alaska has adopted the sharing limitations in 34 C.F.R. Part 99 (FERPA) and 34 C.F.R. 300.123 (regarding confidentiality of personally identifiable information collected for students with disabilities). Alaska Admin. Code tit. 4 § 52.765(a)(2). "Except as provided by this section, a student's standards-based test and alternate assessment results are confidential and may not be disclosed by a district except as provided by 34 C.F.R. Part 99."

Alaska Admin. Code tit. 4 § 06.738(a)

If so, are there exceptions?

None are discussed.

Data Minimization

Are there data retention limits?

In the context of education for children with disabilities and gifted children, if a record containing personally identifiable information is not needed to provide educational services "The district shall destroy the record upon request of the parent. A record of the child's name, address, telephone number, grades, attendance record, classes attended, grade level completed, and year completed must be maintained indefinitely."

Ala. Admin. Code tit. 4 § 52.765(b)

Is de-identification or aggregation of data required?

Alaska does not appear to require de-identification or aggregation. However, Alaska requires the creation of a School District Report Card to the Public, which comprises aggregated student information such as attendance and graduation rates.

Alaska Admin Code. tit. 4 § 06-895.

Security

Does the law mandate specific security practices or creation of a data security program?

Generally, Alaska charges its state agencies to establish procedures that will "protect any confidential, privileged, proprietary, or security information" and "provide a security plan to prevent unintentional or unauthorized addition, modification, deletion, or corruption of electronic records and to ensure routine back-up of essential information."

Alaska Admin. Code. tit. 4 § 59.005

Auditing and Accountability

Must school districts or companies have a CPO?

Yes. Alaska requires that "[e]ach district shall assign one employee the duty to protect the confidentiality of any personally identifiable information and provide each employee who collects, maintains, or uses personally identifiable information with instruction regarding the obligations of the district under" FERPA and 34 C.F.R. 300.123.

Alaska Admin. Code tit. 4 § 52.765(a)

Is there a complaint process when the law has been violated?

Alaska does not appear to provide a specific complaint process.

Individual Participation

Can parents/students opt-out of data collection or sharing?

Alaska does not appear to address the ability of parents or students to opt-out of data collection or sharing.

Arizona

Applicable Laws

Title 15 of Ariz. Rev. Stat. Ann. governs "Education"

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Educational Records" are defined as "those official records, files and data directly related to a student and maintained by the school or local education agency, including records encompassing all the material kept in the student's cumulative folder such as:

- general identifying data;
- records of attendance and of academic work completed;
- records of achievement and results of evaluative tests;
- health data;
- disciplinary status;
- test protocols; and
- individualized education programs."

Ariz. Rev. Stat. Ann. § 15-1911

While the relevant state laws discuss "educational records" regularly, other than the above section, this term is not formally defined.

"Student Data"

Arizona defines "student level data" as records relating to "the calculation of funding for public education, the determination of student academic progress as measured by student testing programs in this state, state and federal reporting requirements and other duties prescribed to the department of education or the state board of education by law."

Does not include data related to:

- student behavior;
- discipline;
- criminal history;
- medical history;
- religious affiliation;
- personal physical descriptors;
- or family information not authorized by the parent or guardian of the pupil or otherwise required by law."

Ariz. Rev. Stat. Ann. § 15-1042(J)

Use Limitations

Is sharing student data with third parties limited or prohibited?

Student transcripts are not to be released to representatives of postsecondary institutions, the militia of Arizona, or the armed services of the United States without student consent.

Ariz. Rev. Stat. Ann § 15-142(B)

Arizona's department of education specifically "may contract with a third party" to develop and implement an education learning and accountability system to maintain and report student level data.

Ariz. Rev. Stat. Ann § 15-249

If so, are there exceptions?

In addition to those detailed in FERPA, certain exceptions such as the release of an educational report to the department of juvenile corrections, are found in Ariz. Rev. Stat. Ann. § 15-141

Data Minimization

Are there data retention limits?

Arizona adopts FERPA's requirements for collection maintenance or disclosure of student educational records compiled by the department of education.

Ariz. Rev. Stat. Ann § 15-1045(A)

Is de-identification or aggregation of data required?

Arizona requires the use of a unique "pupil identifier" in its database that is "not identifiable by anyone other than officials maintaining the education database."

Ariz. Rev. Stat. Ann § 15-1045(C)

Security

Is there a mandated data security program or specific security protocols?

The department of education must implement "proper security measures . . . to ensure confidentiality and integrity of the education database," maintain personally identifiable information in a confidential manner that is outside of the public record, and secure its education database from breaches.

Ariz. Rev. Stat. Ann § 15-1045(B)

Auditing and Accountability

Must school districts or companies have a CPO?

There is no requirement for a CPO; however, Arizona has created a data governance commission of individuals from across its educational institutions, which is tasked with identifying and evaluating data usage, privacy and security.

Ariz. Rev. Stat. Ann. § 15-249.01

Is there a complaint process for student and/or parents when the law has been violated?

Yes. Any person who suspects a school district or charter has knowingly violated FERPA or the Privacy Act can notify the principal of the charter school or superintendent of the school district. If the matter is not resolved within sixty days after the notice, the person may file a complaint with the superintendent of public instruction, who may then notify the U.S. Department of Education if the superintendent of the district or principal of the charter school fails to correct the violation wihin 60 days.

Ariz. Rev. Stat. Ann § 15-142(c)

Individual Participation

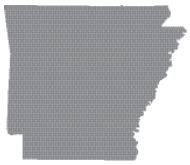
Are parents/students able to opt-out of data collection or sharing?

Arizona does not appear to provide a

Arizona
(continued)

mechanism by which students may opt-out of data collection or sharing.

Arkansas



Applicable Laws

Title 6 of Ark. Code. Ann. governs "Education" Particularly Ark. Code. Ann. § 6-18-109, which codifies Arkansas' Student Online Personal Information Protection Act

Definitions

"Educational Records"

No clear definition, but each school district must maintain a permanent student record as outlined by the state Department of Education.

Ark. Code. Ann. § 6-18-109

"Student Data"

The subsection on the Arkansas Academic Challenge Scholarship Program (postsecondary education), defines "personally identifiable student data" as "any information that, alone or in combination with other available information, is linked or linkable to a specific student that would allow a reasonable person in the student's school community to identify the student with reasonable certainty."

Ark. Code. Ann. § 6-85-204

"Covered information" means "personally identifiable information or materials regarding a public school student in this state" including: name, email address, home address, telephone number, discipline records, test results, special education data, juvenile dependency records, grades, medical or health records, social security number, biometric information, socioeconomic information, political affiliations, religious information, student identifiers, search activity; photos, voice recordings; or geolocation information.

Ark. Code Ann. § 6-18-109

Use Limitations

Is sharing student data with third parties limited or prohibited?

SOPIPA limits the use and dissemination of student data by owners (or "operators") of internet websites, online services, and online and mobile applications that are designed, marketed, and used primarily for public school purposes and are operating in that capacity.

Ark. Code. Ann. § 6-18-109

If so, are there exceptions?

Disclosure limitations do not apply if parties have the "affirmative consent" of the school, student, parent or guardian, in response to clear and conspicuous notice of the use or disclosure. Additionally, aggregated or deidentified covered information may also be used in otherwise impermissible circumstances. The section "does not apply to general audience websites, services, or applications, even if login credentials created on the operator's service are used to access those general audience websites…"

Ark. Code Ann. § 6-18-109

Data Minimization

Are there data retention limits?

Limits on retention are unclear; however:

- Permanent student records shall be maintained by each school district until the student receives a high school diploma or its equivalent.

  Ark. Code Ann. § 6-18-901.

- To receive state foundation funding aid, a school district must keep pupil attendance records in their original form as public records for a period of 3 years after the school term has ended.

  Ark. Code. Ann. § 6-20-2305(f) (5); see also § 6-18-213(a)(1).

- Records containing additional information must be created and maintained for 3 years, along with basic attendance records, for those students who leave school without graduating.

  Ark. Code Ann. § 6-18-214

- Operators must delete "public school student's covered information within a reasonable time frame if the school or district requests deletion" of such information under their control.

  Ark. Code Ann. § 6-18-109

Is de-identification or aggregation of data required?

No de-identification or aggregation is required, but entities subject to the provisions can use de-identified or aggregated covered information in certain ways such as to develop and improve educational products, to show the effectiveness of the products, including the marketing thereof, and to develop or improve educational services.

Ark. Code Ann. § 6-18-109(g)

Security

Is there a mandated data security program or specific security protocols?

Under SOPIPA, operators must implement and "maintain reasonable security measures that are appropriate to the nature of the covered information obtained and protect the covered information from unauthorized access, destruction, use, modification, or disclosure."

Ark. Code Ann. § 6-18- 109

Auditing and Accountability

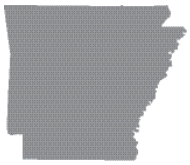
Must school districts or companies have a CPO?

Arkansas does not appear to have codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

A process exists, but only for vocational

Arkansas
(continued)



and technical schools; “any student may file a written complaint with the director on the forms prescribed and furnished by the director for that purpose if the student has reason to believe he or she is suffering loss or damage resulting from (1) the failure of a school to perform agreements made with the student, or (2) an admissions representative’s misrepresentations in enrolling the student.”

Ark. Code Ann. § 6-51-616

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Arkansas does not appear to have a codified ability to opt-out of data collection or sharing.

California

Applicable Laws

Cal. Educ. Code § 10804;

Cal. Educ. Code § 49061;

Cal. Educ. Code § 49063;

Cal. Educ. Code § 49064;

Cal. Educ. Code § 49070;

Cal. Educ. Code § 49073;

Cal. Educ. Code § 49074;

Cal. Educ. Code § 49075;

Cal. Educ. Code § 49076;

Cal. Educ. Code § 60900; and

Cal. Bus. & Prof. Code § 22584 (applies to operators of online services with actual knowledge that the service is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes).

Definitions

"Pupil record"

Any item of information directly related to an identifiable pupil, other than directory information, that is maintained by a school district or required to be maintained by an employee in the performance of his or her duties whether recorded by handwriting, print, tapes, film, microfilm, or other means. It does not include informal notes related to a pupil compiled by a school officer or employee that remain in the sole possession of the maker and are not accessible or revealed to any other person except a substitute. Cal. Educ. Code § 49061(b)

Includes a pupil's health record. Cal. Educ. Code § 49062.

Legislation passed in 2014 defines it as both of the following: (i) any information directly related to a pupil that is maintained by the local educational agency; and (ii) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational agency employee. It does not include certain types of deidentified information. Cal. Educ. Code § 49073.1(c).

"Directory information"

One or more of the following items:

- pupil's name;
- address;
- telephone number;
- date of birth;
- email address;
- major field of study;
- participation in officially recognized activities and sports;
- weight and height of members of athletic teams;
- dates of attendance;
- degrees and awards received; and
- the most recent previous public or private school attended by the pupil.

Cal. Educ. Code § 49061(c).

"Pupil-generated content"

Materials created by a pupil, including, but not limited to:

- essays
- research reports
- portfolios
- creative writing
- music or other audio files
- photographs; and
- account information that enables ongoing ownership of pupil content.

It does not include pupil responses to a standardized assessment where such possession "would jeopardize the validity and reliability of that assessment."

Cal. Educ. Code § 49073.1(c).

"Covered information"

Anything that is created by a student, is descriptive of a student, or otherwise identifies a student. This definition includes, but is not limited to:

- information in the student's educational record or email account
- first and last name;
- home address;
- telephone number;
- email address; or
- other information that allows physical or online contact;
- discipline records;
- rest results;
- special education data;
- juvenile dependency records;
- grades;
- evaluations;
- criminal records;
- medical records;
- health records;
- social security number;
- biometric information;
- disabilities;
- socioeconomic information;
- food purchases;
- political affiliations;
- religious information;
- text messages;
- documents;
- student identifiers;
- search activity;
- photos;
- voice recordings; or
- geolocation information.

Cal. Bus. & Prof. Code § 22584.

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes. A school district shall not permit access to pupil records to a person except under the following circumstances:

- With written parental consent;

California (continued)

- Under judicial order;
- Access to those particular records is relevant to the legitimate educational interests of the requester and the requester falls within a specified category of persons, including school officials and employees of the local educational agency, officials and employees of other public schools or school systems, and other state and local officials; or
- Other specified exceptions, such as releasing pupil records to organizations or agencies in connection with the application of a student for financial aid, accrediting associations, or organizations conducting studies for, or on behalf of, educational agencies or institutions.

Cal. Educ. Code § 49076(a), 49077.

Additional restrictions for operators, subject to certain exceptions, under Cal. Bus. & Prof. Code § 22584.

If so, are there exceptions?

School districts are allowed to grant access to pupil records with written consent from the pupil's parents. The written consent must specify "the records to be released" and identify "the party or class of parties to whom the records may be released." The authorized recipient must be notified that the transmission of the student's information to others without the written consent of the parent is prohibited. The consent notice shall be permanently kept with the record file.

Cal. Educ. Code § 49075.

School districts are allowed to provide "statistical data from which no pupil may be identified" to public agencies, private nonprofit colleges, universities, or educational research and development organizations, "when such actions would be in the best educational interests of pupils."

Cal. Educ. Code § 49074.

School districts may enter into a contract with a third party for either or both of the following purposes: (1) to provide services, including cloud-based services, for the digital storage, management, and retrieval of pupil records; or (2) "to provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use pupil records in accordance with certain contractual provisions."

Contractual provisions must include:

- a statement that the pupil records continue to be the property of the school district,
- a prohibition against the third party using pupil records for purposes other than those specifically permitted by the contract, and
- a description of the actions the third party will take to ensure the security and confidentiality of pupil records.

Cal. Educ. Code § 49073.

Directory information may be released according to local policy as to any pupil or former pupil. However, notice shall be given at least on an annual basis of the categories of information that the school district plans to release and of the recipients.

Cal. Educ. Code § 49073.

Data Minimization

Are there data retention limits?

School districts shall establish, maintain, and destroy pupil records according to regulations adopted by the State Board of Education. Cal. Educ. Code § 49062.

No pupil records shall be destroyed unless a parent successfully challenges the content accuracy of a pupil record. Cal. Educ. Code § 49062.

There are specific retentions and deletion provisions for records containing information gathered from social media. Information gathered from social media must be destroyed within one year after a pupil turns 18 years of age or within one year after the pupil is no longer enrolled in the school district, county office of education, or charter school, whichever occurs first. Cal. Educ. Code § 49073.6.

An operator must delete student covered information if the school or district requires deletion of data under the control of the school or district. Cal. Bus. & Prof. Code § 22584.

Is de-identification or aggregation of data required?

Not required, but there are definitions of deidentified information. Cal. Educ. Code § 49073.1(d).

Security

Is there a mandated data security program or specific security protocols?

School districts shall establish, maintain, and destroy pupil records according to regulations adopted by the State Board of Education.

Cal. Educ. Code § 49062.

A log or record shall be maintained for each pupil's record which lists all persons, agencies, or organizations requesting or receiving information from the record and the legitimate interests therefor. This log can only be accessed by certain people.

Cal. Educ. Code § 49064.

There are contractual requirements with third parties.

Cal. Educ. Code § 49073.

To secure privileged or confidential data from unauthorized disclosure, each state agency and school district is required to develop security procedures or devices by which unauthorized personnel cannot access data contained in the system.

Cal. Educ. Code § 49076.

An operator must implement and

California
(continued)

maintain reasonable security procedures and practices appropriate to the nature of the covered information, and protect that information from unauthorized access, destruction, use, modification, or disclosure.

Cal. Bus. & Prof. Code § 22584.

Auditing and Accountability

Must school districts or companies have a CPO?

California has a statewide Chief Information Officer, who is responsible for a number of duties. However, there is no specific requirement for school districts or companies receiving student data. Cal. Educ. Code § 10804.

Is there a complaint process for student/parents when the law has been violated?

There is no specified complaint process regarding a data privacy violation. School districts are required to notify parents (in writing) of their rights when a student first enrolls in school and again at the beginning of the school year. The notice is intended to alert the parents of the information available to them about their student including the right of the parent to access student records, the procedures for challenging the content of student records, and the right of the parent to file a complaint with the concerning an alleged failure by the school district to comply with federal law.

Cal. Educ. Code § 49063.

Is there a private right of action?

Not specified by statute.

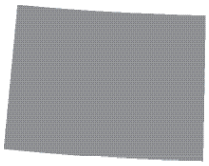
Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Directory information shall not be released regarding a pupil if a parent of that pupil has notified the school district that the information shall not be released.

Cal. Educ. Code § 49073.

Colorado



Applicable Laws

Title 22 of Colo. Rev. Stat. governs "Education"

Key provisions include:

The Data Reporting and Technology Act, codified at Colo. Rev. Stat. § 22-2 Part 3, including the Student Data Protection, Accessibility, Transparency, and Accountability Act of 2014 (C.R.S. § 22-2-309);

C.R.S. § 22-1-123

C.R.S. § 22-2-106.5

C.R.S. § 22-5-119

Definitions

"Educational Records"

"As used in this section, 'education records' and 'directory information' shall have the same meanings as those terms are defined in the federal 'Family Educational Rights and Privacy Act of 1974', as amended, 20 U.S.C. sec. 1232g and 'education records' shall include an individualized education program."

Colo. Rev. Stat. § 22-1-123(1)

FERPA defines "education records" as those records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution.

"Covered Information" or "Student Data"

(I) "Student data" means data that is collected and stored by the department at the individual student level and included in a student's educational record.

(II) "Student data" includes:

(A) State-administered assessment results, including participation information;

(B) Courses taken and completed, credits earned, and other transcript information;

(C) Course grades and grade point average;

(D) Grade level and expected graduation year;

(E) Degree, diploma, credential attainment, or other school exit information;

(F) Attendance and mobility information between and within Colorado school districts;

(G) Special education data and special education discipline reports limited to objective information that is sufficient to produce the federal Title IV annual incident report;

(H) Date of birth, full name, gender, race, and ethnicity; and

(I) Program participation information required by state or federal law.

Colo. Rev. Stat. § 22-2-309(e)

Use Limitations

Is sharing student data with third parties limited or prohibited?

Districts "shall not release the education records of a student to any person, agency, or organization without the prior written consent" of a parent or legal guardian, except as otherwise permitted in 20 U.S.C. sec. 1232g(b).

Colo. Rev. Stat. § 22-1- 123(3)

Districts "shall not release directory information to any person, agency, or organization without first complying with the provisions of 20 U.S.C. sec. 1232g(a)(5)(B) related to allowing a parent or legal guardian to prohibit such release without prior consent."

Colo. Rev. Stat. § 22-1-123(4)

The state board of education (BOE) shall implement guidelines as to how information may be properly shared with a third party, "including by instituting requirements on the recipient entities to not share students' personally identifiable information (PII) with any further third parties and to destroy the personally identifiable information with it is no longer needed."

Colo. Rev. Stat. § 22-2-309

If so, are there exceptions?

Yes. The exceptions found in FERPA at 20 U.S.C. §§ 1232g(b) and 1232g(a)(5)(B) apply.

Data Minimization

Are there data retention limits?

The state board of education is statutorily charged to create a security plan that specifically includes "Data retention and disposition policies, which must include specific criteria for identifying when and how the data will be destroyed."

Colo. Rev. Stat. § 22-2-309(3)(b)(V)

Is de-identification or aggregation of data required?

Principals of each public school must submit an annual report to the state board of education that details information such as attendance records, dropout rates, and code of conduct information. The portion of this report detailing the number of acts of sexual violence on school grounds, in a school vehicle, or at a school activity or sanctioned event must be reported in the aggregate and not include any personally identifiable information.

Colo. Rev. Stat. § 22-32-109.1(2)(b)(IX)

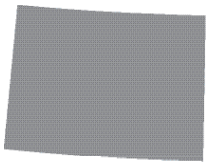
Security

Is there a mandated data security program or specific security protocols?

Each school district must maintain the confidentiality of individual student's "addresses, telephone numbers, medical psychological, sociological, and scholastic achievement data."

Colo. Rev. Stat. § 22-32-109.3(1)

Colorado
(continued)



The state BOE is charged with developing a detailed security plan, which includes guidelines for accessing student data, privacy compliance standards, security breach planning, notice, and procedures, data retention and disposition policies, as well as staff training regarding the policies, among other matters.

Colo. Rev. Stat. § 22-2-309

Auditing and Accountability

Must school districts or companies have a CPO?

Colorado does not appear to statutorily require a CPO.

Is there a complaint process for student/parents when the law has been violated?

Colorado does not appear to have a codified right to a complaint process with respect to student privacy matters.

Is there a private right of action?

See above.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

A school district must obtain the consent of a parent or legal guardian, in compliance with the FERPA requirements, before releasing directory information or education records of a student to any person, agency, or organization. Furthermore, parental consent must be obtained prior to giving a student any survey, assessment, analysis, or evaluation intended to reveal information, either personally identifiable or not, about matters such as political affiliations, sexual behavior, social security number, or religious practices, among other matters of the student or their parent or legal guardian.

Colo. Rev. Stat. § 22-1-123

Connecticut

Applicable Laws

Title 10 of the Conn. Gen. Stat. governs "Education and Culture"

Title 10a of the Conn. Gen. Stat. governs "State System of Higher Education"

Specific provisions include: Conn. Gen. Stat. § 10-10a; 10-15b; 10-15f; 10a-42h

Definitions

"Educational Records"

Pursuant to Connecticut's codification of the Interstate Compact on Educational Opportunity for Military Children, "Educational records" means "the official records, files, and data directly related to a student and maintained by the school or local education agency, including, but not limited, to records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs."

Conn. Gen. Stat. § 10-15f

"Covered Information" or "Student Data"

With respect to the section related to higher education, "confidential student data or records includes, but is not limited to, personally identifiable information, as defined in the regulations implementing the Family Educational Rights and Privacy Act of 1974" ("FERPA").

Conn. Gen. Stat. § 10a-42h

Use Limitations

Is sharing student data with third parties limited or prohibited?

The Department of Education (DOE) is charged with the development of a state-wide school information system, which tracks student data while maintaining its confidentiality. The system shall assign each student with a unique student identifier. The data included in this system shall include, but not be limited to, the primary language spoken at the student's home, transcripts, and attendance and mobility, among other things. This information is to be shared with the data systems of public institutions of higher education in the state. Further, the system database of student information shall not be considered a public record for the purposes of Conn. Gen. Stat. § 1-120.

Conn. Gen. Stat. § 10-10a.

However, note that under Conn. Gen. Stat. § 1-120, educational records "which are not subject to disclosure under FERPA" are excluded. The DOE shall provide data maintained in the information system to a full-time permanent employee of a nonprofit organization organized and operated for educational purposes, following a written request from such an individual.

Conn. Gen. Stat. § 10-10a(c)(3)(H)

Parents or legal guardians of a minor student are entitled to knowledge of and access to all educational, medical, or similar records maintained in a student's cumulative record other than professional communications between a teacher or nurse and a student regarding any alcohol or drug abuse or problem of that student. Additionally, schools will produce school or student records in connection with a subpoena issued by a competent authority.

Conn. Gen. Stat. § 10-15b

The Board of Regents for Higher Education shall institute policies to "prohibit public institutions of higher education from disclosing identifying information of undergraduate students at such institutions to credit card issuers unless such institutions have provided such students with notice of and the opportunity to opt out of such disclosure in accordance with the regulations adopted by the United States Department of Education pursuant to FERPA."

Conn. Gen. Stat. § 10a-44b

If so, are there exceptions?

See above.

Data Minimization

Are there data retention limits?

Connecticut does not appear to codify such limits.

Is de-identification or aggregation of data required?

Connecticut does not appear codify such requirements.

Security

Is there a mandated data security program or specific security protocols?

The Department of Education's state-wide school information system "shall be designed for the purpose of establishing a standardized electronic data collection and reporting protocol that will... maintain the confidentiality of individual student and staff data."

Conn. Gen. Stat. § 10-10a

Auditing and Accountability

Must school districts or companies have a CPO?

Connecticut does not appear codify such a requirement.

Is there a complaint process for student/parents when the law has been violated?

Connecticut has a formal complaint system that is not specific to student privacy, implemented pursuant to Conn. Gen. Stat. §§ 10-4a & 4b.

Is there a private right of action?

This ability to bring a complaint is

Connecticut
(continued)

granted to "[a]ny resident of a local or regional school district, or parent or guardian of a student enrolled in the public schools of such school district."

Conn. Gen. Stat. § 10-4b(a)

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

In the context of higher education, students must be given the opportunity to opt out of the disclosure of their information is a public institution of higher education is to disclose identifying information of undergraduate students to credit card issuers.

Conn. Gen. Stat. § 10a-44b

Delaware

Applicable Laws

Title 14 of Del. Code Ann. Governs "Educations"

Note: Title 14, Chapter 81A, known as the "Student Data Privacy Protection Act" comes into effect on August 1, 2016. These provisions are to be found at 14 Del. Code Ann. §§ 8101A-8106A.

Definitions

"Educational Records"

"'Educational Record' shall mean personally identifiable student information maintained by an education agency or institution, as defined by the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) and its implementing regulations at 34 CFR part 99, and the Individuals with Disabilities Education Act, 20 U.S.C. 1400 et seq. and its implementing regulations, and other applicable federal and state privacy and confidentiality laws."

14 Del. Admin. Code § 294

"'Education record' means an education record as defined in FERPA."

14 Del. Code Ann. § 8102A

In the context of postsecondary education, "student records" means "all those documents that are necessary to provide a meaningful record of student performance and financial aid."

14 Del. Code. Ann. § 8530

"Covered Information" or "Student Data"

"Student Data" is defined at 14 Del. Code Ann. § 8102A(16), and includes, but is not limited to, such categories of data as student performance information and personally identifiable information created or provided by a student or a patent to an employee or agent of the Department of Education, a school district, a school, or an operator of a website, application, or service used for K-12 school purposes.

Starting August 1, 2017, the most recently updated version of the Student Data Privacy Protection Act becomes effective and includes the following definition of "student data" for all uses starting from the effective date:

Personally identifiable information or materials, in any media or format, that meets any of the following:

a. is student performance information;

b. is created or provided by a student or parent to an employee or agent of the Department, school district, or school;

c. is created or provided by a student or parent to an operator in the course of the student's or parent's use of the operator's site, service, or application for K-12 school purposes;

d. is created or provided by an employee or agent of a school district or school, to an operator;

e. is gathered by an operator through the operation of a site, service, or application described in paragraph (10)a. of this section and can be used to distinguish or trace the identity of the student, or is linked to information that can be used to distinguish or trace the identity of the student, including information in the student's education record or email; the student's name, in whole or in part; residential or other address that allows physical contact; telephone number; online contact information; discipline records; test results; special education data; juvenile dependency records; criminal records; medical records; health records; Social Security number; passport number; student identification number or other student identifier; driver's license number; state identification card number; alien registration number; geolocation data; biometric information; disability status; socioeconomic information; food purchases; political affiliations; religious information; text messages; instant messages; documents; search activity; photos; voice recordings; or video recordings.

14 Del. Code Ann. § 8102A

Use Limitations

Is sharing student data with third parties limited or prohibited?

A third party operator of an application, website, or service used for K-12 school purposes is prohibited from engaging in targeted advertising arising from the use of student data, use information gathered to amass a profile of a student except in furtherance of K-12 school purposes, sell student data, or otherwise disclose student data.

14 Del. Code Ann. § 8105A

If so, are there exceptions?

There are limits to a third party's disclosure of student data limitations codified at 14 Del. Code Ann. § 8105A(4 – 6). Examples include disclosure for legitimate research purposes, to ensure legal or regulatory compliance, and to a service provider (given that provider agrees to certain contractual obligations regarding the student data).

Further, the Student Data Privacy Protection Act is not to be construed to apply to general audience websites, services, or applications, limit the authority of law enforcement to access content and student data as authorized by law or pursuant to a court order, prohibit operators from marketing educational products to parents (where the marketing is not derived from the use of student data), or prevent the Department of Education, a school district or a school from recommending educational materials, products, or services for K-12 purposes to a student or the student's family, among other

Delaware
(continued)

limitations.

14 Del. Code Ann. § 8106A

Data Minimization

Are there data retention limits?

A third party operator shall delete "a student's data within a reasonable timeframe not to exceed 45 calendar days if a school district or school requests deletion of data under the control of the school district or school."

14 Del. Code Ann. § 8104A

Is de-identification or aggregation of data required?

There is no requirement to de-identify or aggregate student data, but 14 Del. Code Ann. § 8102A defines "aggregate student data" and "de-identified data," and 14 Del. Code Ann. § 8105A explains permissible uses of aggregated or de-identified data on the part of a third party operator of an application, website, or service used for K-12 school purposes.

Security

Is there a mandated data security program or specific security protocols?

A third party operator shall implement "and maintain reasonable security procedures and practices appropriate to the nature of the student data to protect that information from unauthorized access, destruction, use, modification, or disclosure, which shall, at a minimum, comply with the Department of Technology and Information's (DTI) Cloud and Offsite Hosting Policy and include the terms and conditions set forth in the DTI's Cloud and Offsite Hosting Template for Non-Public Data."

14 De. Code Ann. § 8104A

Auditing and Accountability

Must school districts or companies have a CPO?

Delaware does not appear to have codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

Delaware does not appear to have codified such a process.

Is there a private right of action?

See above.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Delaware does not appear to have codified an ability to opt-out of data collection or sharing.

District of Columbia

Applicable Laws

D.C. Code Ann. § 38-203

D.C. Code Ann. § 38-355

D.C. Code Ann. § 38-651.08

D.C. Code Ann. § 38-1802.04

D.C. Code Ann. § 38-1853.10

D.C. Code Ann. § 38-2609

Definitions

"Educational Records"

No explicit definition.

"Covered Information" or "Student Data"

No explicit definition.

Use Limitations

Is sharing student data with third parties limited or prohibited?

No specific statute prohibits the sharing of student data with third parties.

D.C. does require that the Office of the State Superintendent of Education ("OSSE") develop and implement "a longitudinal educational data warehouse system ("EDW system")" that maintains the confidentiality of individual student and staff data, in accordance with D.C. and federal confidentiality laws, rules, and regulations.

The EDW system is to be used by all providers of public education, including the OSSE, the University of the District of Columbia (UDC), public schools, public charter schools, publicly funded educational programs, policymakers, institutions of higher education, and researchers.

The EDW system shall be used to compile, analyze, research, and organize student, teacher, and school-level data to: (1) Facilitate compliance with D.C. and federal reporting requirements; (2) Aid in local and state-level policymaking and programming; and (3) Improve information exchanges.

The State Superintendent can request that necessary data pertaining to students, teachers, and school levels be submitted to the OSSE for the purpose of constructing, updating, or maintaining the EDW system.

The OSSE shall ensure that a unique identifier is assigned to every student and teacher in a public school, public charter school or publicly funded educational program, as well as every student of UDC. The unique identifier will be assigned the first time that a student receives educational services from a provider of public education in D.C.

D.C. Code Ann. § 38-2609

Schools are also required to create and maintain a list of students with valid medication action plans, including the emergency contact information for each student. These lists may be distributed among appropriate school employees. In addition, schools shall maintain accurate records of all incidents where medication was administered to a student in an emergency circumstance.

D.C. Code Ann. § 38-651.08

An accurate daily record of the attendance of all minors shall be kept by each institution, and shall be open for inspection at all times by the Board, the Superintendent of Schools, school attendance officers, or other persons authorized to enforce D.C. Code Ann. § 38-203.

The Ombudsman for Public Education shall not: (1) Disclose personally identifiable information (PII) regarding a student without the specific written consent of the student or parent, as required by federal and local law… or (3) Disclose the identity of any person who brings a complaint or provides information to the Ombudsman without the person's consent, unless the Ombudsman determines that disclosure is unavoidable or necessary to further the ends of an investigation.

D.C. Code Ann. § 38-355

Each public charter school shall submit an annual report to the eligible chartering authority that approved its charter, which includes student data. The data shall not identify the individuals to whom the data pertains. Public charter schools shall also provide to the Board of Education student enrollment data necessary to comply with its census record requirements.

D.C. Code Ann. § 38-1802.04

Each eligible entity receiving scholarship funds must submit a yearly report to the Secretary regarding the activities carried out with the funds during the preceding year. These reports many not contain PII. Reports to parents may only contain the PII of their child.

D.C. Code Ann. § 38-1853.10

If so, are there exceptions?

Not specified by statute.

Data Minimization

Are there data retention limits?

There is no specific statute limiting how long data can/should be retained.

Security

Is there a mandated data security program or specific security protocols?

There is no specific statutory mandate for a data security program or specific security protocols.

Is there required de-identification or aggregation of data?

There is no specific statute requiring de-identification or aggregation of data.

District of Columbia
(continued)

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

There is no specific CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

D.C has no specific statute involving a complaint process.

Is there a private right of action?

D.C. has no specific statute that indicates a private right of action.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

D.C. has no specific statute allowing parents/students to opt-out of data collection or sharing.

Florida

Applicable Laws

Title XLVIII of Fla. Stat. contains the "Education Code"

Key provisions:

Fla. Stat. § 1002.22 details the rights of students and parents with respect to education records, explaining that these rights mirror those found in the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) ("FERPA").

See also Fla Stat. § 1002.221- 222

Definitions

"Educational Records"

"Education records" in Florida are defined as they are in FERPA.

Fla. Stat. § 1002.221(1)

"Covered Information" or "Student Data"

In the context of private schools, "Student records" are defined as "those records, files, documents, and other materials that contain information directly related to students that are maintained by a private school or by a person acting for such institution and that are accessible to other professional personnel to facilitate the instruction, guidance, and educational progress of students. Information contained in student records shall be classified as follows:

a. Permanent information, which includes verified information of clear educational importance, containing the following: student's full name and any known changes thereto due to marriage or adoption; authenticated birthdate, place of birth, race, and sex; last known address of student; names of student's parents; name and location of last school attended; number of days present and absent; date enrolled; date withdrawn; courses taken and record of achievement; and date of graduation or program achievement.

b. Temporary information, which includes verified information subject to change, containing, but not limited to, the following: health information, standardized test scores, honors and activities, personal attributes, work experience, teacher and counselor comments, and special reports."

Fla. Stat. § 1002.42(a)(2)

Use Limitations

Is sharing student data with third parties limited or prohibited?

"An agency or institution, as defined in § 1002.22, may not release a student's education records without the written consent of the student or parent to any individual, agency, or organization, except in accordance with and as permitted by" FERPA.

Fla. Stat. § 1002.221(2)(a)

If so, are there exceptions?

In addition to those exceptions found in FERPA, education records may be released to the Auditor General and the Office of Program Policy Analysis of Florida, which must use and maintain the records in accordance with FERPA. Further, education records may be released without written consent of the student or parent pursuant to an interagency agreement among the Department of Juvenile Justice, the school, law enforcement authorities, and other signatory agencies in certain circumstances.

Fla. Stat. § 1002.221(2) (b-c)

Data Minimization

Are there data retention limits?

An agency or institution may not "collect, obtain, or retain information on the political affiliation, voting history, religious affiliation, or biometric information of a student or a parent or sibling of the student."

Fla. Stat. § 1002.222

Security

Is there a mandated data security program or specific security protocols?

"Each principal shall maintain a permanent cumulative record for each student enrolled in a public K-12 school. Such record shall be maintained in the form, and contain all data, prescribed by rule by the State Board of Education. The cumulative record is confidential and exempt from the provisions of § 119.07(1) and is open to inspection only as provided in Chapter 1002."

Fla. Stat. § 1003.25

Is there required de-identification or aggregation of data?

Florida does not appear to codify this as a requirement.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Florida does not appear to codify this as a requirement.

Is there a complaint process for student/parents when the law has been violated?

"If any official or employee of an institution refuses to comply with this section, the aggrieved parent or student has an immediate right to bring an action in circuit court to enforce his or her rights by injunction. Any aggrieved parent or student who receives injunctive relief may be awarded attorney fees and court costs."

Fla. Stat. § 1002.22(4); see also Fla. Stat. § 1002.225(3)

Is there a private right of action?

See above.

Florida
(continued)

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

"An agency or institution, as defined in s. 1002.22, may not release a student's education records without the written consent of the student or parent to any individual, agency, or organization, except in accordance with and as permitted by the FERPA."

Fla. Stat. 1002.221(2)(a)

Georgia

Applicable Laws

Title 20 of Ga. Code Ann. Governs "Education"

The "'Student Data Privacy, Accessibility, and Transparency Act," (effective as of July 1, 2016) codified at Ga. Code Ann. § 20-2-660 – 20-2-668;

See also Ga. Code Ann. § 20-2-281; 20-2-320

Definitions

"Educational Records"

"Education record" is defined as "an education record as defined in the Family Educational Rights and Privacy Act (FERPA) and its implementing regulations, 20 U.S.C. Section 1232g and 34 C.F.R. Part 99.3. An education record does not include the types of student data excepted in FERPA, does not include student data collected by an operator when it is used for internal operations purposes, does not include student data that is not formatted for or expected to be accessed by school, local board of education, or department employees, nor does it include student data that a local board of education determines cannot reasonably be made available to the parent or eligible student."

Ga. Code Ann. § 20-2-662(4)

"Covered Information" or "Student Data"

"Student data" is defined as "information regarding a K-12 student who is a resident of this state that is collected and maintained at the individual student level in this state."

Ga. Code Ann. § 20-2-662(12) (this provision continues on to provide a non-exhaustive list of categories of information that are to be considered "student data")

"Student personally identifiable data" or "student personally identifiable information" or "personally identifiable information" means "student data that personally identifies a student that, alone or in combination, is linked to information that would allow a reasonable person who does not have personal knowledge of the relevant circumstances to identify the student."

Ga. Code Ann. § 20-2-662(13)

Use Limitations

Is sharing student data with third parties limited or prohibited?

With respect to the Georgia Board of Education's (BOE) student assessment program, the "results of individual student performance on academic skills assessment instruments… shall be confidential and may be released only in accordance with [FERPA]."

Ga. Code Ann. § 20-2-281

With respect to the state-wide comprehensive educational information system, all "data maintained for this system shall be used for educational purposes only. In no case shall information be released by an authorized educational agency which would violate the privacy rights of any individual student or employee. Information released by an authorized educational agency in violation of the privacy rights of any individual student or employee shall subject the authorized educational agency to all penalties under applicable state and federal law."

Ga. Code Ann. § 20-2- 320(c)

Without the written consent of a student over the age of 18 or a minor student's parent or legal guardian, an operator of websites, online services, or applications used for K-12 purposes ("operator") may not use student data to engage in behaviorally targeted advertising, amass a profile of a student (except in furtherance of K-12 school purposes), sell a student's data, or otherwise disclose a student's data (with some exceptions).

Ga. Code Ann. § 20-2-666(a)

Certain categories of information are not to be reported to the Georgia Department of Education (DOE) by the local boards of education unless required by state or federal law. These categories of information include juvenile delinquency records, medical or health records, political affiliation and voting history of a student or their family, and religious affiliation of a student or their family, among others.

Ga. Code Ann. § 20-2-665

If so, are there exceptions?

An operator may disclose student data to a third party in certain circumstances such as to service providers (where those providers are bound to certain contractual obligations), to respond to or participate in the judicial process, or for legitimate research purposes, as detailed at Ga. Code Ann. § 20-2-666.

Data Minimization

Are there data retention limits?

The DOE is charged with implementing data retention and disposal policies.

Ga. Code Ann. § 20-2-664(4)(D)

An operator must delete "a student's data within a reasonable timeframe not to exceed 45 days if the school or local board of education requests deletion of data under" the given board's control.

Ga. Code Ann. § 20-2-666(b)

Security

Is there a mandated data security program or specific security protocols?

The chief privacy officer is responsible for "[e]stablishing department-wide policies necessary to assure that the use of technologies sustains, enhances, and does not erode privacy protections relating to the use, collection, and disclosure of student data."

Georgia (continued)

Ga. Code Ann. § 20-2-663(a)(1)

The Department of Education shall "[d]evelop a detailed data security plan for the state data system" which includes features such as, but not exclusively, privacy and security audits, data retention and disposal policies, and guidance for local boards of education to implement effective security practices that are consistent with those of the state data system."

Ga. Code Ann. § 20-2-664(4)

An operator must "implement and maintain reasonable security procedures and practices appropriate to the nature of the student data to protect that information from unauthorized access, destruction, use, modification, or disclosure."

Ga. Code Ann. § 20-2-666(b)

Is there required de-identification or aggregation of data?

With respect to the Georgia BOE's student assessment program, "Overall student performance data shall be disaggregated by ethnicity, sex, socioeconomic status, disability, language proficiency, grade level, subject area, school, system, and other categories determined by policies established by the Office of Student Achievement."

Ga. Code Ann. § 20-2- 281

"Any information collected over the state-wide comprehensive educational information system" that is not stored in an individual student or personnel record "shall be made available to the Governor and the House and Senate Appropriations Committees, the House Committee on Education, the Senate Education and Youth Committee, the House Committee on Higher Education, and the Senate Higher Education Committee, except information otherwise prohibited by statute." Data included in individual student or personnel records shall be extracted and "made available in nonindividual record format for use" by the Governor, General Assembly committees, and agencies other than authorized educational agencies."

Ga. Code Ann. § 20-2- 320(c)

"Student performance data shall be made available to the public, with appropriate interpretations, by the State BOE, the Office of Student Achievement, and local school system. The information made available to the public shall not contain the names of individual students or teachers."

Ga. Code Ann. § 20-2-281(o)

Further, the terms "aggregate student data" and "de-identified data" are defined in Ga Code Ann. § 20-2-662.

Operators may use aggregate or de-identified data in certain ways, such as to improve the operator's offerings or to demonstrate the effectiveness of the operator's products or services, including in marketing.

Ga. Code Ann. § 20-2-666(e)

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

"The State School Superintendent shall designate a senior department employee to serve as the chief privacy officer of the department to assume primary responsibility for data privacy and security policy."

Ga. Code Ann. § 20-2-663

Is there a complaint process for student/parents when the law has been violated?

"The department shall develop model policies and procedures for a parent or [student over the age of 18] to file a complaint with a local school system regarding a possible violation of rights under this article or under other federal or state student data privacy and security laws."

Ga. Code Ann. § 20-2-667(g)

Is there a private right of action?

"Nothing in this Code section shall authorize any additional cause of action beyond the process described in this Code section or as otherwise authorized by state law."

Ga. Code Ann. § 20-2-667(h)

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

For an operator to use student data, unless the use falls within one of the specific exceptions enumerated by statute, a student over the age of 18 or a parent or legal guardian of a minor student must give written consent.

Ga. Code Ann. § 20-2-666

Hawaii

Applicable Laws

Title 18 of Haw Rev. Stat. governs "Education"

Title 8, Chapter 34 of the Haw. Code R. governs the "Protection of Educational Rights and Privacy of Students and Parents"

Definitions

"Educational Records"

Pursuant to Hawaii's codification of the Interstate Compact on Educational Opportunity for Military Children, "Education records" are defined as "those official records, files, and data directly related to a student and maintained by the school or appropriate education agency, including records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs."

Haw. Rev. Stat. § 311D-1

When sharing data between themselves, the Hawaii Department of Education, the University of Hawaii, the Department of Labor and Industrial Relations, and other state agencies must share said data "in a manner that safeguards the confidentiality of student education records, as defined by the federal Family Educational Rights and Privacy Act."

Haw. Rev. Stat. § 27-7(b)

"Education records" is defined as "all records, files, documents, and other materials maintained by the department" of education, which contain information directly related to an individual student."

Haw. Code R. § 8-34-3 (certain categories of information are excepted from inclusion under this provision)

"Covered Information" or "Student Data"

Hawaii does not appear to have defined these terms.

Use Limitations

Is sharing student data with third parties limited or prohibited?

The Board of Education "shall establish educational reporting standards that shall include minimum standards for reporting fiscal, personnel, and student data, by means of electronic transfer of data files from charter schools to" the Hawaii Department of Education.

Haw. Rev. Stat. § 302D-23

"The department shall not make accessible nor release any education records or personally identifiable information (PII) without the written consent of" a student over the age of 18 or a parent.

Haw. Code R. § 8-34-14(a)

If so, are there exceptions?

Exceptions to Haw. Admin. R. § 8-34-14(a) include release of education records or PII without written consent to department officials who have a legitimate educational interest in the records, authorized representatives of relevant entities in the federal government, or in connection with an emergency if the knowledge of that information is necessary to protect the health and safety of that student or other persons.

Haw. Code R. § 8-34- 14(a)

Data Minimization

Are there data retention limits?

"The department may destroy or expunge any records of a student when they no longer are appropriate, relevant, or required under department rules. However, when an eligible student or parent requests access to the records, access shall be granted prior to the destruction of records."

Haw. Code R. § 8-34-7

Security

Is there a mandated data security program or specific security protocols?

Hawaii does not appear to have codified a security program or specific security protocols.

Is there required de-identification or aggregation of data?

For charter schools, performance provisions within the charter contract are to be based on a performance framework that includes indicators such as student academic proficiency and growth, attendance, and postsecondary readiness. This framework "shall require the disaggregation of all student performance data by major student subgroups."

Haw. Rev. Stat. § 302D-16

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Hawaii does not appear to have a codified CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

There is a codified complaint/hearing process to review and challenge the contents of a student record. A codified process to address privacy violations or data breaches is not apparent.

Haw. Code R. §§ 8-34-10 – 8-34-13.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Hawaii
(continued)

Regarding the education records of their children, parents have the right to: "(1) Inspect, review, challenge or obtain copies thereof, (2) allow others to review them; and (3) grant permission for their release." Further, these rights transfer to the student when they turn 18.

Haw. Code R. § 8-34-4

"The department shall not make accessible nor release any education records or [PII] without the written consent of" a student over 18 or a parent.

Haw. Code R. § 8-34-14(a)

"The department shall give public notice of the kinds of directory information on students that are available. Within ten days after the notice, a parent may request that certain data be withheld except with prior consent."

Haw. Code R. § 8-34- 14(g)

Idaho

Applicable Laws

The key provision for student privacy in Idaho is Idaho Code Ann. § 33-133

Definitions

"Educational Records"

"Student educational record" is defined as "all information directly related to a student and recorded and kept in the data system as that term is defined in this section. Provided, however, that the following shall not be kept as part of a student's permanent educational record: daily assignments, homework, reports, chapter tests or similar assessments, or other schoolwork that may be considered daily or weekly work. A student educational record may include information considered to be personally identifiable."

Idaho Code Ann. § 33-133(1)(k)

"A student's educational record shall not include: (1) juvenile delinquency records and criminal records unless required in paragraph (k) of this subsection; (2) medical and health records; (3) student social security number; (4) student biometric information; (5) gun ownership records; (6) sexual orientation; (7) religious affiliation; (8) except for special needs and exceptional students, any data collected pursuant to a statewide assessment via affective computing, including analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart rate variability, pulse, blood volume, posture and eye tracking, any data that measures psychological resources, mind sets, effortful control, attributes, dispositions, social skills, attitudes or intrapersonal resources."

Idaho Code Ann. § 33-133(1)(j)(ii)

"Covered Information" or "Student Data"

"Student data" is defined as "data collected and/or reported at the individual student level included in a student's educational record."

Idaho Code Ann. § 33-133(1)(j)

"Student data" includes: "(1) state and national assessment results, including information on untested public school students; (2) course taking and completion, credits earned and other transcript information; (3) course grades and [GPA]; (4) [DOB], grade level and [expected graduation date/cohort]; (5) degree, diploma, credential attainment and other school exit information such as general educational development and drop-out data; (6) attendance and mobility; (7) [data required to calculate the federal four year adjusted secondary cohort graduation rate]; (8) [discipline reports limited to objective information sufficient to produce the federal annual incident reports, disciplinary reports for children with disabilities or reports including students involved with firearms; (9) remediation; (10) special education data; (11) demographic data and program participation information; and (12) [Files, data, etc.], containing a student's educational record [stored in or transmitted through a cloud computing service]."

Idaho Code Ann. § 33-133(1)(j)(i)

Use Limitations

Is sharing student data with third parties limited or prohibited?

The Idaho Board of Education ("BOE") shall ensure that access "to student data in the student data system shall be restricted to:" (1) authorized BOE and state department of education (DOE) staff, and "vendors who require such access to perform their assigned duties"; (2) school districts, their vendors, and public postsecondary staff who require such access to perform their assigned duties; (3) students and their parents or legal guardians; and (4) the authorized staff of other state agencies" as required by law and/or defined by interagency data-sharing agreements. All such agreements are summarized yearly in a BOE report submitted to the legislature's education committees.

Idaho Code Ann. § 33-133(3)(b)(i)

The BOE shall ensure that all school districts, schools, and other similar institutions contractually bind vendors to the use of aggregate data, or to use individual students' data only in specific ways, and only with written permission from a student's parent or legal guardian.

Idaho Code Ann. § 33-133(3) (b)(vi)

If so, are there exceptions?

Idaho's limits and prohibitions on sharing student data with third parties are intended to comply with the Family Educational Rights and Privacy Act.

Idaho Code Ann. § 33-133(3)(b) and (3)(e)

Data Minimization

Are there data retention limits?

The BOE shall ensure "that any contract entered into by [the BOE or DOE] includes provisions requiring and governing data destruction dates and specific restrictions" on data use.

Idaho Code Ann. § 33-133(3)(b)(iv)

Security

Is there a mandated data security program or specific security protocols?

TThe BOE shall develop "a detailed data security plan," with required elements as detailed in Idaho Code Ann. § 33-33(3)(d).

The BOE shall develop, and each district and public charter school shall adopt, a model policy governing data collection, access, security and use.

Idaho Code Ann. § 33-133(7)

Is there required de-identification or

Idaho
(continued)

aggregation of data?

The BOE shall provide "that public reports or responses to record requests shall include aggregate data only."

Idaho Code Ann. § 33-133(3)(b)(ii)

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

There is no clear CPO requirement; however, "all decisions relating to the collection and safeguarding of student data shall be the responsibility of the executive office of the BOE."

Idaho Code Ann. § 33-133(2)

Is there a complaint process for student/parents when the law has been violated?

There is not a codified complaint process for student privacy and data breaches.

Is there a private right of action?

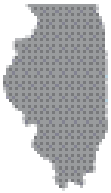
Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

As noted in Idaho Code Ann. § 33-133(3)(b), for the majority of third party collections, use of individual student records requires parental consent.

Illinois



Applicable Laws

Illinois School Student Records Act 105 ILCS 10/1-10

Definitions

"Educational Records"

"School Student Record" is defined in 105 ILCS 10/2 (d) as "any writing or other recorded information concerning a student and by which a student may be individually identified, maintained by a school or at its direction or by an employee of a school, regardless of how or where the information is stored."

"Student Permanent Record" is defined in 105 ILCS 10/2 (e) as "the minimum personal information necessary to a school in the education of the student and contained in a school student record. Such information may include the student's name, birth date, address, grades and grade level, parents' names and addresses, attendance record, and such other entries as the State Board may require or authorize."

"Student Temporary Record" means all information contained in a school student record but not contained in the student permanent record. Such information may include family background information, intelligence test scores, aptitude test scores, psychological and personality test results, teacher evaluations, and other information of clear relevance to the education of the student, all subject to regulations of the State Board…. the student temporary record shall include information regarding serious disciplinary infractions that resulted in expulsion, suspension, or the imposition of punishment or sanction. For purposes of this provision, serious disciplinary infractions means: infractions involving drugs, weapons, or bodily harm to another."

105 ILCS 10/2 (f)

"Covered Information" or "Student Data"

Illinois does not appear to have defined these terms.

Use Limitations

Is sharing student data with third parties limited or prohibited?

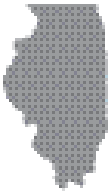
105 ILCS 10/4 (f) provides, "student temporary records shall not be disclosed except as provided in Section 5 or 6 or by court order."

ISSRA provides that "[n]othing contained in this Act shall prohibit the publication of student directories which list student names, addresses and other identifying information and similar publications which comply with regulations issued by the State Board.

If so, are there exceptions?

105 ILCS 10/6 creates a broad prohibition on release of school student records subject to several enumerated exceptions: (1) to a parent or student or person specifically designated as a representative by a parent; (2) to an employee or official of the school or school district or State Board with current demonstrable educational or administrative interest in the student, in furtherance of such interest; (3) to the official records custodian of another school within Illinois or an official with similar responsibilities of a school outside Illinois, in which the student has enrolled, or intends to enroll, upon the request of such official or student; (4) to any person for the purpose of research, statistical reporting, or planning, provided that such research, statistical reporting, or planning is permissible under and undertaken in accordance with the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g); (5) pursuant to a court order, provided that the parent shall be given prompt written notice upon receipt of such order of the terms of the order, the nature and substance of the information proposed to be released in compliance with such order and an opportunity to inspect and copy the school student records and to challenge their contents; (6) to any person as specifically required by State or federal law; (7) subject to regulations of the State Board, in connection with an emergency, to appropriate persons if the knowledge of such information is necessary to protect the health or safety of the student or other persons; (8) to any person, with the prior specific dated written consent of the parent designating the person to whom the records may be released, provided that at the time any such consent is requested or obtained, the parent shall be advised in writing that he has the right to inspect and copy such records, to challenge their contents, and to limit any such consent to designated records or designated portions of the information contained therein; (9) to a governmental agency, or social service agency contracted by a governmental agency, in furtherance of an investigation of a student's school attendance pursuant to the compulsory student attendance laws of this State, provided that the records are released to the employee or agent designated by the agency; (10) to those SHOCAP committee members who fall within the meaning of "state and local officials and authorities," as those terms are used within the meaning of the Family Educational Rights and Privacy Act, for the purposes of identifying serious habitual juvenile offenders and matching those offenders with community resources pursuant to Section 5-245 of the Juvenile Court Act of 1987, but only to the extent that the release, transfer, disclosure, or dissemination is consistent with the Family Educational Rights and Privacy Act; (11) to the Department

Illinois
(continued)



of Healthcare and Family Services in furtherance of the requirements of Section 2-3.131, 3-14.29, 10-28, or 34-18.26 of the School Code or Section 10 of the School Breakfast and Lunch Program Act; or (12) to the State Board or another State government agency or between or among State government agencies in order to evaluate or audit federal and State programs or perform research and planning, but only to the extent that the release, transfer, disclosure, or dissemination is consistent with the federal Family Educational Rights and Privacy Act.

Data Minimization

Are there data retention limits?

105 ILCS 10/4 (f) states, "[a] school may maintain indefinitely anonymous information from student temporary records for authorized research, statistical reporting or planning purposes, provided that no student or parent can be individually identified from the information maintained."

Security

Is there a mandated data security program or specific security protocols?

Each school is required to have an "official records custodian," who is responsible for "maintenance, care and security of all school student records, whether or not such records are in his personal custody or control."

105 ILCS 10/4 (a)

Further, the records custodian "shall take all reasonable measures to prevent unauthorized access to or dissemination of school student records.

105 ILCS 10/4 (b)

Is there required de-identification or aggregation of data?

Schools are only authorized to maintain records of "anonymous information from student temporary records" and only for "authorized research, statistical reporting or planning purposes, provided that no student or parent can be individually identified from the information maintained."

105 ILCS 10/4 (f)

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Illinois does not appear to have codified the requirement for a CPO.

Is there a complaint process for student/parents when the law has been violated?

Illinois does not appear to have codified a complaint process addressing privacy violations or student data breaches.

Is there a private right of action?

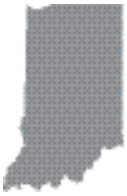
Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Illinois does not appear to have codified such an ability.

Indiana



Applicable Laws

Note: Indiana does not currently have a large amount of statutory language regarding student data and privacy.

Definitions

"Educational Records"

"Education Records" is defined as "information that is recorded by a nonpublic or public school and concerns a student who is or was enrolled in the school."

Ind. Code § 20-33-7-1

Pursuant to the codification of the Interstate Compact on Educational Opportunity for Military Children, "educational records" are defined as "official records, files, and data that are directly related to a student and maintained by a school or local education agency. The term includes general identifying data, records of attendance and academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs."

Ind. Code § 20-38-3-2

"Covered Information" or "Student Data"

Indiana does not appear to have defined these terms.

Use Limitations

Is sharing student data with third parties limited or prohibited?

"A school corporation or other entity to which the education records privacy provisions of the federal Family Educational Rights and Privacy Act (20 U.S.C. 1232g) apply may disclose or report on the education records of a child, including personally identifiable information contained in the education records, without the consent of the child's parent under the following conditions:

- The disclosure or reporting of education records is to a state or local juvenile justice agency.
- The disclosure or reporting relates to the ability of the juvenile justice system to serve, before adjudication, the student whose records are being released.
- The juvenile justice agency receiving the information certifies, in writing, to the entity providing the information that the agency or individual receiving the information has agreed not to disclose it to a third party, other than another juvenile justice agency, without the consent of the child's parent."

Ind. Code § 20-33-7-3

If so, are there exceptions?

N/A

Data Minimization

Are there data retention limits?

Indiana does not appear to have codified such limits.

Security

Is there a mandated data security program or specific security protocols?

Indiana does not appear to have codified such a mandate.

Is there required de-identification or aggregation of data?

Indiana does not appear to have codified such a requirement.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Indiana does not appear to have codified the requirement for a CPO.

Is there a complaint process for student/parents when the law has been violated?

Indiana does not appear to have codified a complaint process addressing privacy violations or student data breaches.

Is there a private right of action?

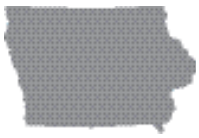
Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Indiana does not appear to have codified such an ability.

Iowa



Applicable Laws

Title VII of the Iowa Code governs "Education and Cultural Affairs"

Other key provisions: Iowa Code § 22.7

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "education records" or "educational records" are defined as "those official records, files, and data directly related to a student and maintained by the school or local education agency, including but not limited to records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs."

Iowa Code § 256H.1

"Covered Information" or "Student Data"

Iowa does not appear to define these terms.

Use Limitations

Is sharing student data with third parties limited or prohibited?

"The following public records shall be kept confidential, unless otherwise ordered by a court, by the lawful custodian of the records, or by another person duly authorized to release such information: Personal information in records regarding a student, prospective student, or former student maintained, created, collected or assembled by or for a school corporation or educational institution maintaining such records."

Iowa Code § 22.7

"Notwithstanding any provision of law or rule to the contrary, personal information in records regarding a child receiving competent private instruction or independent private instruction pursuant to this chapter, which are maintained, created, collected, or assembled by or for a state agency, shall be kept confidential in the same manner as personal information in student records maintained, created, collected, or assembled by or for a school corporation or educational institution in accordance with section 22.7, subsection 1."

Iowa Code § 299A.11

The Director of the Department of Education shall "Develop and implement a comprehensive management information system designed for the purpose of establishing standardized electronic data collections and reporting protocols that facilitate compliance with state and federal reporting requirements, improve school-to-school and district-to-district information exchanges, and maintain the confidentiality of individual student and staff data. The system shall provide for the electronic transfer of individual student records between schools, districts, postsecondary institutions, and the department. The director may establish, to the extent practicable, a uniform coding and reporting system, including a statewide uniform student identification system."

Iowa Code § 256.9

If so, are there exceptions?

Iowa Code § 22.7 is "not to be construed to prohibit a postsecondary education institution from disclosing to a parent or guardian information regarding a violation of a federal, state, or local law, or institutional rule or policy governing the use or possession of alcohol or a controlled substance if the child is under the age of twenty-one years and the institution determines that the student committed a disciplinary violation with respect to the use or possession of alcohol or a controlled substance regardless of whether that information is contained in the student's education records. This subsection shall not be construed to prohibit a school corporation or educational institution from transferring student records electronically to the department of education, an accredited nonpublic school, an attendance center, a school district, or an accredited postsecondary institution in accordance with section 256.9, subsection 48."

Iowa Code § 22.7

Data Minimization

Are there data retention limits?

Iowa does not appear to have codified a data retention limit.

Security

Is there a mandated data security program or specific security protocols?

Iowa Code § 22.7 details the types of records that are to "be kept confidential, unless otherwise ordered by a court, by the lawful custodian of the records, or by another person duly authorized to release such information." These include are detailed above in the "Use Limitations" section.

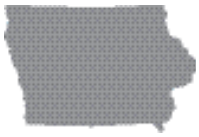
The Director of the Iowa Department of Education shall approve, "coordinate, and supervise the use of electronic data processing by school districts, area education agencies, and merged areas."

Iowa Code § 256.9

Is there required de-identification or aggregation of data?

Iowa does not appear to have codified a requirement for this.

Iowa
(continued)



Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Iowa does not appear to have codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

Iowa does not appear to have codified a complaint proves for privacy violations or student data breaches.

Is there a private right of action?

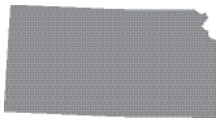
Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Iowa does not appear to have codified an ability to opt-out.

Kansas



Applicable Laws

Chapter 72 of Kan. Stat. Ann governs "Schools"

Key Provisions: Student Data Privacy Act (Kan. Stat. Ann. §§ 72-6215 – 72-6223)

Definitions

"Educational Records"

"School records" means transcripts, grade cards, the results of tests, assessments or evaluations, and all other personally identifiable records, files, and data directly related to a pupil.

Kan. Stat. Ann. § 72-5386

"Covered Information" or "Student Data"

Kan. Stat. Ann. § 72-6216 defines the following:

"Student data" means the following information contained in a student's educational record: State and national assessment results, including information on untested students; course taking and completion; credits earned and other transcript information; course grades and grade point average; date of birth, grade level and expected date of graduation; degree, diploma, credential attainment and other school exit information such as general education development and drop-out data; attendance and mobility; data required to calculate the federal four-year adjusted cohort graduation rate, including sufficient exit and drop-out information; remediation; special education data; demographic data and program participation information; and any other information included in a student's educational record.

"Personally identifiable student data" means student data that, alone or in combination, is linked or linkable to a specific student and would allow a reasonable person to identify the student with reasonable certainty.

"Directory information" means a student's name, address, telephone listing, participation in officially recognized activities and sports, weight and height if the student is a member of an athletic team, and degrees, honors or awards received.

Use Limitations

Is sharing student data with third parties limited or prohibited?

Pursuant to Kan. Stat. Ann. § 72-6217, student data submitted to and maintained by the statewide longitudinal student data system may only be disclosed in accordance with the provisions of the section. Permissible disclosures codified in the section include disclosure to the student or parent or legal guardian of the student, disclosure to the authorized personnel of a state agency or to a service provider acting under a data-sharing agreement with the educational agency, disclosure of aggregate data to a governmental entity or to an audit or research organization, and disclosure of directory information to an enhancement vendor providing photography services, class ring services, yearbook publishing services, or other substantially similar services.

If so, are there exceptions?

See above.

Data Minimization

Are there data retention limits?

When student data is transferred to another agency or to a service provider pursuant to a data-sharing agreement, "the student data shall be destroyed when no longer necessary for the purposes of the data-sharing agreement or upon expiration of the data-sharing agreement, whichever occurs first." A service provider "engaged to perform a function of instruction may retain student transcripts as required by applicable laws and rules and regulations. Destruction shall comply with the NISTSP800-88 standards of data destruction."

Kan. Stat. Ann. § 72-6217

Security

Is there a mandated data security program or specific security protocols?

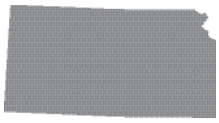
"Every board shall adopt a policy in accordance with the student data privacy act and applicable federal laws and regulations to protect the right of privacy of any student, or pupil and such pupil's family regarding personally identifiable records, files and data directly related to such student or pupil… Such procedures shall provide for: (1) Means by which any student or parent of a pupil… may inspect and review any records or files directly related to the student or pupil; and (2) restricting the accessibility and availability of any personally identifiable records or files of any student or pupil and preventing disclosure thereof unless made upon written consent of such student or parent of such pupil…"

Kan. Stat. Ann. § 72-6214

Is there required de-identification or aggregation of data?

"Every board shall adopt a policy in accordance with the student data privacy act and applicable federal laws and regulations to protect the right of privacy of any student, or pupil and such pupil's family regarding personally identifiable records, files and data directly related to such student or pupil… Such procedures shall provide for: (1) Means by which any student or parent of a pupil… may inspect and review any records or files directly related to the student or pupil; and (2) restricting the accessibility and availability of any personally identifiable

Kansas
(continued)



records or files of any student or pupil and preventing disclosure thereof unless made upon written consent of such student or parent of such pupil…"

Kan. Stat. Ann. § 72-6214

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Kansas does not appear to have a codified CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

A complaint process with respect to student privacy is not apparent, but Kan. Stat. Ann. § 72-6221 does codify a notification process for breaches or unauthorized disclosures of student data.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Kansas does not appear to have codified an ability to opt-out of data collection or sharing.

Kentucky

Applicable Laws

Title XIII of the Ky. Rev. Stat. Ann. Governs "Education"

Key Provisions: Kentucky Family Education Rights and Privacy Act (Ky. Rev. Stat. Ann. §§ 160.700 – 160.730)

Definitions

"Educational Records"

"Education record" means data and information directly relating to a student that is collected or maintained by educational institutions or by a person acting for an institution, including academic records and portfolios; achievement tests; aptitude scores; teacher and counselor evaluations; health and personal data; behavioral and psychological evaluations; and directory data recorded in any medium including handwriting, magnetic tapes, film, video, microfiche, computer-generated and stored data, or data otherwise maintained and used by the educational institution or a person acting for an institution.

"Education record" shall not include:

- Records of instructional, supervisory, and assisting administrative personnel which are in the sole possession of the maker and are not accessible or revealed to any other person except a substitute for any of those persons;
- Records maintained by a law enforcement unit of the educational institution that were created by that law enforcement unit for the purpose of law enforcement;
- In the case of persons who are employed by an educational agency or institution but who are not in attendance at that agency or institution, records made and maintained in the normal course of business which relate exclusively to that person in the person's capacity as an employee and are not available for use for any other purpose; or
- Records on a student who is 18 years of age or older, which are made, used, or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional for treatment of the student, and are not available to anyone other than persons providing this treatment, except a physician or other appropriate professional of the student's choice.

Ky. Rev. Stat. Ann. § 160-700

"Covered Information" or "Student Data"

"Directory information" means the student's name, address, telephone listing, date and place of birth, participation in school recognized sports and activities, height and weight of members of athletic teams, dates of attendance, awards received, major field of study, and the most recent previous educational agency or institution attended by the student, contained in education records in the custody of the public schools.

Ky. Rev. Stat. Ann. § 160-700

"Student data" means any information or material, in any medium or format, that concerns a student and is created or provided by the student in the course of the student's use of cloud computing services, or by an agent or employee of the educational institution in connection with the cloud computing services. Student data includes the student's name, e-mail address, e-mail messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student.

Ky. Rev. Stat. Ann. § 365.734

"Education data" means the following data relating to student performance from early childhood learning programs through postsecondary education: College and career readiness; Course and grade; Degree, diploma, or credential attainment; Demographic; Educator; Enrollment; Financial aid; High school equivalency diploma; Remediation; Retention; State and national assessments; Transcripts; Vocational and technical education information; and any other data impacting education deemed necessary by the office

Ky. Rev. Stat. Ann. § 151B.131

Use Limitations

Is sharing student data with third parties limited or prohibited?

Education records of the students of public educational institutions are deemed confidential and shall not be disclosed, or the contents released, except under the circumstances described in Ky. Rev. Stat. Ann. § 160.720.

Ky. Rev. Stat. Ann. § 160.705

"All student academic records shall be confidential and shall not require a student's Social Security number to identify the student… and shall not be released by any public supported institution of higher education in Kentucky, to any person, organization, institution, group, or agency, except with the express consent of the individual student. This confidentiality shall apply only to student academic records, including, but not limited to, official transcript of grades."

Ky. Rev. Stat. Ann. § 164.283

If so, are there exceptions?

Unless a parent or a student over the age of 18 gives consent for the release of educational records, reports, or identifiable information, such materials may only be released or disclosed under certain circumstances including, but not limited to, other school officials with legitimate educational interests and purposes, individuals or organizations conducting legitimate

Kentucky (continued)

studies, surveys, and data collection in such a manner so as not to permit personal identification of students or parents, and to accrediting organizations enlisted to carry out accrediting functions.

Ky. Rev Stat. Ann. § 160.720

Additionally, student directory information may be disclosed where an educational institution gives notice of the categories of directory information to be disclosed and after a reasonable amount of time has not been informed by a parent or a student over the age of 18 that any or all of the information designated may not be released without prior consent.

If an educational institution provides access to its campus or its student directory information to persons or groups which make students aware of occupational or educational options, the board shall provide access on the same basis to official recruiting representatives of: (1) The Armed Forces of the United States; (2) The Kentucky Air National Guard; (3) The Kentucky Army National Guard; and (4) The service academies of the Armed Forces of the United States.

Ky. Rev. Stat. Ann. § 160.725

Ky. Rev. Stat. Ann. § 164.283(3 – 9) contains certain limited exceptions to the requirement of confidentiality absent express consent to disclose student academic records by public postsecondary educational institutions.

Data Minimization

Are there limits on how long data can/should be retained?

"School officials shall take precautions to protect and preserve all education records, including records generated and stored in the education technology system. School officials shall:

- Retain for a minimum period of one (1) week a master copy of any digital, video, or audio recordings of school activities without editing, altering, or destroying any portion of the recordings, although secondary copies of the master copy may be edited; and
- Retain for a minimum of one (1) month in an appropriate format, a master copy of any digital, video, or audio recordings of activities that include, or allegedly include, injury to students or school employees without editing, altering, or destroying any portion of the recordings."

Ky. Rev. Stat. Ann. § 160.705

Security

Is there a mandated data security program or specific security protocols?

Ky. Rev. Stat. Ann. § 160.705, as detailed above, mandates the preservation of educational records and requires school officials to retain unedited master copies of video and audio recordings of school activities for a minimum of one week, and requires that any such materials that included or allegedly include injury to students or school employees be preserved unedited for a minimum of one month.

"The Kentucky Department of Education shall develop protocols for student records within the student information system which: (1) Provide notice to schools receiving the records of prior offenses described in KRS 610.345 committed by a student transferring to a new school or district; and (2) Protect the privacy rights of students and parents guaranteed under the federal Family Educational Rights and Privacy Act."

Ky. Rev. Ann. Stat. § 158.448

Is there required de-identification or aggregation of data?

"The duties of the Office for Education and Workforce Statistics shall be to: (1) Oversee and maintain the warehouse of education data and workforce data in the Kentucky Longitudinal Data System; (2) Develop de-identification standards and processes using modern statistical methods. . ."

Ky. Rev. Stat. Ann. § 151B.133

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Kentucky does not appear to have a codified CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

"Parents or eligible students may challenge the content of a student record to ensure that the record or report is not inaccurate, misleading, or otherwise in violation of privacy or other rights of the student. The right to challenge shall also provide the opportunity for rebuttal to, and the correction, deletion, or expunction of, any inaccurate, misleading, or inappropriate information."

Ky. Rev. Stat. Ann. § 160.730 (this provision goes on to detail the process by which the challenge is to take place)

Is there a private right of action?

See above.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

If a school intends to disclose student directory information, a student over the age of 18 or a minor student's parent has the ability to opt-out of any or all of this information disclosure following the school providing notice of the categories of directory information it intends to disclose.

Ky. Rev. Stat. Ann. § 160.725

Further, parents or "eligible students

Kentucky
(continued)

shall be informed of the rights of privacy and confidentiality accorded student education records. The educational institution shall determine the means and method of notice and adopt written policies consistent with the state law."

Ky. Rev. Stat. Ann. § 160.710

Louisiana

Applicable Laws

La. Revised Statutes §§ 17-3911, 17-3912; 17-3913; 17-3914; 17-2100.8; 17-81; 51-1954

Definitions

"Educational Records"

Used but undefined under Louisiana statute. Statutory annotations discussing education records under Family Educational Rights and Privacy Act (20 U.S.C. 1232(g) ("FERPA") suggests that the FERPA definition of "Education Record" is relied upon.

"Covered Information" or "Student Data"

The Louisiana statutes covering student education information refers to personally identifiable student information in setting forth the limitations on the disclosure of this information by public school system to the school board or public or private entities. The statute defines "personally identifiable information" ("PII") as information about an individual that can be used on its own or with other information to identify, contract, or locate a single individual, including but not limited to the following: any information that can be used to distinguish or trace an individual's identity such as full name, social security number, date and place of birth, mother's maiden name, or biometric records; any other information that is linked or linkable to an individual such as medical, educational, financial and employment information; and two or more pieces of information that separately or when linked together can be used to reasonably ascertain the identity of the person.

La. Revised Statute § 17-3914.

Also, under the Louisiana statutes "the Legislature declares that all [PII] is protected as a right to privacy under the Constitution of Louisiana and the Constitution of the United States."

La. Revised Statute § 17-3914

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes. No official or employee of a city, parish, or other local public school system shall provide personally identifiable student information to any member of the school board or to any other person or public or private entity.

La. Revised Statute § 17-3914 (C)(2)

In addition, no city, parish, or other local public school system, local or state governmental agency, public or private entity, or any person with access to personally identifiable student information shall sell, transfer, share, or process any student data for use in commercial advertising, or marketing, or any other commercial purpose.

La. Revised Statute § 17-3914 (J)

Further no person or public or private entity shall access a public school computer system on which student information is stored. No official or employee of a public school system shall authorize access to such a computer system to any person or public or private entity (except in a few limited situations set forth below).

La. Revised Statute § 17-3914 (D)(1)

If so, are there exceptions?

Yes, an official or employee may, in accordance with State Board of Elementary and Secondary Education regulation or applicable state and federal law:

- Provide a student's identification number and aggregate data to the local school board, the state Department of Education ("DOE"), or the State Board of Elementary and Secondary Education solely for the purpose of satisfying state and federal reporting requirements.
- Provide to the state DOE, for the purpose of satisfying state and federal assessment, auditing, funding, monitoring, program administration, and state accountability requirements, information from which enough PII has been removed such that the remaining information does not identify a student and there is no basis to believe that the information alone can be used to identify a student. No official or employee of the state DOE shall share such information with any person or public or private entity located outside of Louisiana, other than for purposes of academic analysis of assessments.
- Provide PII regarding a particular student to any person or public or private entity if the sharing of the particular information with the particular recipient of the information has been authorized in writing by the parent or legal guardian of the student, or by a student who has reached the age of legal majority, or if the information is provided to a person authorized by the state, including the legislative auditor, to audit processes including student enrollment counts. Any recipient of such information shall maintain the confidentiality of such information. Any person who knowingly and willingly fails to maintain the confidentiality of such information shall be subject to penalties.

La. Revised Statute § 17-3914 (C)(2)

Furthermore, a person authorized by the superintendent to maintain or repair the computer system or to provide services that the school system would otherwise provide and a person authorized by the State to audit student records may access a public school computer system or the computer

Louisiana
(continued)

system of a city, parish, or other local public school system on which student information for students at a particular school is stored.

La. Revised Statute § 17-3914 (D)(2) & (3)

In addition, a city, parish, or other local public school board may contract with a private entity for student and other educational services, and pursuant to such contract, student information, including PII and cumulative records, may be transferred to computers operated and maintained by the private entity for such purpose.

La. Revised Statute § 17-3914 (F)

Data Minimization

Are there data retention limits?

The governing authority of each public school, each Louisiana postsecondary educational institution, and the Office of Student Financial Assistance shall destroy all (student) data collected not later than five years after the student graduates, unless otherwise required by state or federal law or regulation.

La. Revised Statute § 17-3914 (K)(4)

In addition, for contractors hired pursuant to La. Revised Statute § 17-3914(F), the contracts must contain a provision for the disposal of all information from the servers of the contractor upon termination of the contract and all information removed from the contractor's servers must be returned to the city, parish or other local public school board.

La. Revised Statute § 17-3914 (F)(3)(k)

The governing authority of each public school, each Louisiana postsecondary educational institution, and the Office of Student Financial Assistance shall destroy all (student) data collected not later than five years after the student graduates, unless otherwise required by state or federal law or regulation.

La. Revised Statute § 17-3914(K)(4)

Security

Is there a mandated data security program or specific security protocols?

A contract pursuant to La. Revised Statute § 17-3914 (F) must include the following requirements regarding the protection of student information:

- guidelines for authorizing access to computer systems on which student information is stored including guidelines for authentication of authorized access.
- privacy compliance standards.
- privacy and security audits performed under the direction of the local school superintendent.
- breach planning, notification, and remediation procedures.
- information storage, retention, and disposition policies.
- disposal of all information from the servers of the contractor upon termination of the contract

La. Revised Statute § 17-3914 (F)(3)

Is there required de-identification or aggregation of data?

Each local public school board must assign a unique student identification number to every student enrolled in a public elementary or secondary school. These numbers shall not include or be based on social security numbers, and students shall retain their number for their entire tenure in Louisiana public elementary and secondary schools.

La. Revised Statute § 17-3914 (C)(3)

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Louisiana does not appear to have a codified CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

Each website for a local education agency and the State DOE is required to provide information on its website about the transfer of personally identifiable student information the describes the process by which parents of students attending public schools may register a complaint related to the unauthorized transfer of personally identifiable student information.

La. Revised Statute § 17-3913.

Is there a private right of action?

Louisiana does not appear to have a codified private right of action.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Beginning in the 8th grade, the governing authority of each public school shall annually, at the beginning of each school year, provide a form to be signed by the parent or legal guardian of each student enrolled in the school, whereby the student's parent or legal guardian may provide consent or deny consent for the collection and disclosure of the student's information.

La. Revised Statute § 17-3914 (K)(3)

Maine

Applicable Laws

Title 20-A of Me. Rev. Stat. governs "Education"

Key Provisions: The Student Information Privacy Act (Me. Rev. Stat. tit. 20-A, § 951, et. seq.)

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Educational records" means those official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to records encompassing all the material kept in the child's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Me. Rev. Stat. tit. 20-A, § 20102

"Covered Information" or "Student Data"

"Student data" means information that is collected and maintained at the individual student level in this State, including, but not limited to:

A. Data descriptive of a student in any media or format, including, but not limited to:

- The student's first and last names;
- The names of the student's parent and other family members;
- The physical address, e-mail address, phone number and any other information that allows contact with the student or the student's family;
- A student's personal identifier, such as the state-assigned student identifier, when used for identification purposes;
- Other indirect identifiers, such as the student's date of birth, place of birth
- and mother's maiden name;
- Results of assessments administered by the State, school administrative unit, school or teacher, including participation information;
- Course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information;
- Attendance and mobility information between and within school administrative units within the State;
- The student's gender, race, and ethnicity;
- Educational program participation information required by state or federal law;
- The student's disability status;
- The student's socioeconomic information;
- The student's food purchases; and
- The student's e-mails, text messages, documents, search activity, photos, voice recordings and geolocation information; and

B. Information that:

- Is created by a student or the student's parent or provided to an employee or agent of the school, school administrative unit, the department or an operator in the course of the student's or parent's use of the operator's website, service or application for kindergarten to grade 12 school ("K-12") purposes;
- Is created or provided by an employee or agent of the school or school administrative unit, including information provided to an operator in the course of the employee's or agent's use of the operator's website, service or application for K-12 purposes; or
- Is gathered by an operator through the operation of an [their] website, service or application for K-12 purposes.

Me. Rev. Stat. tit. 20-A, § 952

"Student personally identifiable information" means student data that, alone or in combination, is linked to a specific student and would allow a reasonable person who does not have knowledge of the relevant circumstances to identify the student.

Me. Rev. Stat. tit. 20-A, § 952

Use Limitations

Is sharing student data with third parties limited or prohibited?

A third party operator may not: use student data to engage in targeted advertising, amass a profile of a student except for K-12 purposes, sell student data, or otherwise disclose student personally identifiable information unless the disclosure is made pursuant to a limited set of exceptions.

Me. Rev. Stat. tit. 20-A, § 953

In addition to specific provisions found in Me. Rev. Stat. tit. 20-A, § 6001, et. seq., PERPA and the federal Individuals with Disabilities Education Act "govern the dissemination of education records and personally identifiable information about students in public schools, private schools approved by the department . . . and private schools recognized by the department as providing equivalent instruction . . ., as well as written notices of intent to provide equivalent instruction through home instruction and all education records of students receiving equivalent instruction through home instruction."

Me. Rev. Stat. tit. 20-A, § 6001

"Education records must be managed in compliance with the federal Family Educational Rights and Privacy Act

Maine (continued)

of 1974, [20 USC § 1232(g), referred to in this section as "FERPA." Personally identifiable information in an educational record that is not directory information may be released to other agencies within State Government, including postsecondary institutions, only under a signed memorandum of understanding requiring compliance with FERPA."

Me. Rev. Stat. tit. 20-A, § 6005

If so, are there exceptions?

Third party operators may disclose student personally identifiable information for limited purposes including, but not limited to, advancing the K-12 school purposes of the operator's website, service, or application, as long as the recipient of the student data disclosed may not further disclose the student data other than to allow or improve operability and functionality of the website, service, or application for use in the classroom, and is legally required to comply with the statute's requirements, responding or participating in the judicial process, and providing the information to a service provider that is bound by certain contractual obligations.

Me. Rev. Stat. Ann. Tit. 20-A, § 953

Data Minimization

Are there data retention limits?

A third party operator receiving student data must delete "student data within 45 days of a school's or school administrative unit's request."

Me. Rev. Stat. Ann. Tit. 20-A, § 953

Security

Is there a mandated data security program or specific security protocols?

A third party operator receiving student data must implement "and maintain reasonable security procedures and practices appropriate to the nature of the student data to protect that data from unauthorized access, destruction, use, modification and disclosure."

Me. Rev. Stat. Ann. Tit. 20-A, § 953

Is there required de-identification or aggregation of data?

"Aggregate student data" means data that is not personally identifiable and that is collected or reported at the group, cohort, or institutional level."

Me. Rev. Stat. tit. 20-A, § 952

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Maine does not appear to have codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

Maine does not appear to have codified such a complaint process for violations of student privacy.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

A public school may not publish on the Internet or provide for publication on the internet any personal information about its students without first obtaining the written approval of those students' parents.

Me. Rev. Stat. tit. 20-A, § 6001

In order to use, sell, or disclose student data in any manner inconsistent with Me. Rev. Stat. tit. 20-A, § 953, a third party operator with access to student data must first obtain written or electronic consent from a student over the age of 18 or a minor student's parent.

Maryland

Applicable Laws

Key Provisions: Md. Code. Ann. Educ. §§ 4-131 (governing third party operators with access to student data), 24-701, et seq. (governing the Maryland Longitudinal Data System)

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Educational records" means those official records, files, and data directly related to a student and maintained by the school or local education agency, including but not limited to records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

Md. Code Ann. Educ. § 7-1303

"Covered Information" or "Student Data"

"Covered information" means information or material that:

- Personally identifies an individual student in this State or that is linked to information or material that personally identifies an individual student in this State; and
- Is gathered by an operator through the operation of a site, a service, or an application.

"Covered information" includes a student's: Educational and disciplinary record; First and last name; Home address and geolocation information; Telephone number; Electronic mail address or other information that allows physical or online contact; Test results, grades, and student evaluations; Special education data; Criminal records; Medical records and health records; Social Security number; Biometric information; Socioeconomic information; Food purchases; Political and religious affiliations; Text messages; Student identifiers; Search activity; Photos; and Voice recordings.

Md. Code Ann. Educ. § 4-131

"Student data" means data relating to student performance. "Student data" includes: State and national assessments; Course-taking and completion; Grade point average; Remediation; Retention; Degree, diploma, or credential attainment; Enrollment; and Demographic data.

"Student data" does not include: Juvenile delinquency records; Criminal and CINA records; Medical and health records; and Discipline records.

Md. Code Ann. Educ. § 24-701

Use Limitations

Is sharing student data with third parties limited or prohibited?

A third party operator with access to covered information may not engage in targeted advertising, use information to make a profile about a student (unless it is in furtherance of a PreK-12 school purpose), sell a student's information, or otherwise disclose covered information unless such disclosure falls within one of the codified exceptions.

An operator may use or disclose covered information where the operator has given "clear and conspicuous notice" and obtained affirmative consent from a student over the age of 18 or a minor student's parent or guardian.

Md. Code Ann. Educ. § 4-131

If so, are there exceptions?

A third party operator may disclose covered information in certain circumstances including, but not limited to, where the disclosure is only made in furtherance of the PreK-12 school purpose of the site, service, or application and the recipient of the information does not further disclose the information and is legally required to comply with the statute, to take precautions against liability, to ensure legal or regulatory compliance, or where the disclosure is to a service provider which is contractually bound in certain ways.

Md. Code Ann. Educ. § 4-131

Data Minimization

Are there data retention limits?

The Maryland Longitudinal Data System Center shall determine the "required disposition of information that is no longer needed."

Md. Code Ann. Educ. § 24-703

The linkage of student data and workforce data for the purposes of the Maryland Longitudinal Data System shall be limited to no longer than 5 years from the date of latest attendance in any educational institution in the State.

Md. Code Ann. Educ. § 24-702

If covered information is under the authority of a public school or local school system in accordance with a contract or an agreement, a third party operator with access to covered information must delete within a reasonable time the covered information if the public school or local school system requests.

Md. Code Ann. Educ. § 4-131

Security

Is there a mandated data security program or specific security protocols?

The Maryland Longitudinal Data System Center shall "Ensure routine and ongoing compliance with the federal Family Educational Rights and Privacy Act and other relevant privacy

Maryland (continued)

laws and policies, including:

- The required use of de-identified data in data research and reporting,
- The required disposition of information that is no longer needed,
- Providing data security, including the capacity for audit trails,
- Providing for performance of regular audits for compliance with data privacy and security standards, and
- Implementing guidelines and policies that prevent the reporting of other potentially identifying data.

Md. Code Ann. Educ. § 24-703

A third party operator with access to covered information shall:

- Protect covered information from unauthorized access, destruction, use, modification, or disclosure;
- Implement and maintain reasonable security procedures and practices to protect covered information; and
- If covered information is under the authority of a public school or local school system in accordance with a contract or an agreement, delete within a reasonable time the covered information if the public school or local school system requests deletion of the covered information.

Md. Code. Ann. Educ. § 4-131

Is there required de-identification or aggregation of data?

See above.

A third party operator with access to covered information may use "aggregated or de-identified covered information:

(i) To develop or improve an educational product or service within any site, service, or application the operator owns; or

(ii) To demonstrate the effectiveness of the operator's products or services; or

(iii) Share aggregated or de-identified covered information for the development or improvement of educational sites, services, or applications."

Md. Code. Ann. Educ. § 4-131

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Maryland does not appear to have codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

While not specific to the student privacy context, the Maryland Office of the Attorney General's Electronic Transaction Education, Advocacy, and Mediation Unit is charged with providing "information and advice to the public on effective ways of handling complaints that involve violations of:

(i) privacy related laws, including identity theft and identity fraud; or

(ii) unlawful conduct or practices in electronic transactions."

Md. Code Ann State Gov't § 6-202

Is there a private right of action?

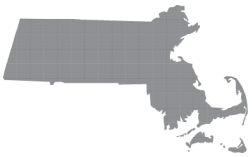
See above.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

In order for a third party operator with access to covered information to be able to use, sell, or disclose that information in a manner not explicitly contemplated by Md. Code Ann. Educ. § 4-131, that operator must first obtain the affirmative consent from a student over the age of 18 or a minor student's parent or guardian.

Massachusetts



Applicable Laws

Title XII of Mass. Gen. Laws governs Education

Mass Gen. Laws ch. 71, § 34D dictates that the board of education shall adopt regulations to govern certain aspects of student privacy.

603 Mass. Code Regs. 23.00, et seq. governs Student Records

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education records" are defined as those official records, files, and data directly related to a student and maintained by the school or local education agency, including, but not limited to, records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

Mass. Gen. Laws ch. 15E, § 1

Each school district shall maintain individual records on every student and employee. Each student record shall contain a unique and confidential identification number, basic demographic information, program and course information, and such other information as the department shall determine necessary.

Mass. Gen. Laws ch. 69, § 1I

Student Record shall consist of the Transcript and the Temporary Record, including all information—recording and computer tapes, microfilm, microfiche, or any other materials—regardless of physical form or characteristics concerning a student that is organized on the basis of the student's name or in a way that such student may be individually identified, and that is kept by the public schools of the Commonwealth.

603 Mass. Code Regs. 23.02

"Covered Information" or "Student Data"

Not defined.

Use Limitations

Is sharing student data with third parties limited or prohibited?

"Except for the provisions of [603 CMR 23.07(4)(a) - 23.07(4)(h)], no third party shall have access to information in or from a student record without the specific, informed written consent of the eligible student or parent." When granting consent, the eligible student or parent has the right to designate which parts of the student record shall be released to the third party."

Except for information described in 603 CMR 23.07(4)(a), personally identifiable information from a student record shall only be released to a third party on the condition that [they] will not permit any other third party to have access to such information without the written consent of the eligible student or parent."

603 Mass. Code Regs. 23.07

If so, are there exceptions?

A school may grant access to student information in certain circumstances including, but not limited to, upon receipt of a court order or lawfully issued subpoena, upon notification by law enforcement that a student or former student is missing, and in connection with a health or safety emergency. Further, a school may release certain categories of directory information provided the school gives public notice of the categories of information it may release and allows eligible students and parents a reasonable time to request that this information not be released without their prior consent.

603 Mass. Code Regs. 23.07

Data Minimization

Are there data retention limits?

The board of education ("BOE") shall adopt regulations covering the maintenance, retention, duplication, storage and periodic destruction of student records by the public elementary and secondary schools.

Mass Gen. Laws ch. 71, § 34D

Student transcripts shall be maintained by the school department and may only be destroyed 60 years following graduation, transfer, or withdrawal from the school system.

603 Mass. Code Regs. § 23.06

Security

Is there a mandated data security program or specific security protocols?

As noted above, the BOE is charged with adopting regulations related to the storage of student records.

Mass Gen. Laws ch. 71, § 34D

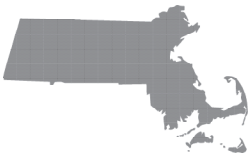
"The principal and superintendent of schools shall insure that student records under their supervision are kept physically secure, that authorized school personnel are informed of the provisions of 603 Mass. Code Regs. 23.00 and Mass. Gen. Laws ch. 71 § 34H, are educated as to the importance of information privacy and confidentiality; and that any computerized systems employed are electronically secure."

603 Code Mass. Regs. 23.05

Is there required de-identification or aggregation of data?

During the time a student is enrolled in a school, the principle or their designee "shall periodically review and destroy misleading, outdated, or irrelevant information contained in the temporary

Massachusetts
(continued)



record" provided that eligible students and/or their parents "are notified in writing and are given opportunity to receive the information or a copy of it prior to its destruction." The temporary record of any student enrolled on or after [8/15/2006] shall be destroyed no later than [7] years after the student transfers, graduates, or withdraws from the school system."

630 Mass. Code Regs. 23.06

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

"The school principal or his/her designee shall be responsible for the privacy and security of all student records maintained in the school. The superintendent of schools or [their] designee shall be responsible for the privacy and security of all student records that are not under the supervision of a school principal, for example, former students' transcripts stored in the school department's central administrative offices or student records of school-age children with special needs who have not been enrolled in a public school."

603 Mass. Code Regs. 23.05

Is there a complaint process for student/parents when the law has been violated?

An eligible student or parent may appeal an unsatisfactory decision of a principal or his/her designee regarding any of the provisions contained in 603 CMR 23.00 to the superintendent of schools. If the appellant finds the decision of the superintendent of schools to be unsatisfactory, the eligible student or parent may appeal the decision to the school committee.

603 Mass. Code Regs. 23.09

Is there a private right of action?

Nothing in 603 Mass. Code Regs. 23.00 shall abridge or limit any right of an eligible student or parent to seek enforcement of 603 Mass. Code Regs. 23.00 or the statutes regarding student records, in any court or administrative agency of competent jurisdiction.

603 Mass. Code Regs. 23.09

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Most of the information in a student's record may only be disclosed to third parties with an eligible student or a parent's consent.

603 Mass. Code Regs. 23.07

Michigan

Applicable Laws

The State School Aid Act of 1979 (Mich. Comp. Laws § 388.1601. et seq.)

The Revised School Code (Mich. Comp. Laws § 380.1, et seq.)

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education(al) records" means: those official records, files, and data directly related to a student and maintained by the school or local education agency, including but not limited to records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

Mich. Comp. Laws § 3.1041

"Covered Information" or "Student Data"

"Pupil directory information" means a pupil's name, address, and, if it is a listed or published telephone number, the pupil's telephone number.

Mich. Comp. Laws § 380.1139

While not formally defined, the Michigan Center for Educational Performance and Information is tasked with creating, maintaining, and enhancing the state's P-20 longitudinal data system. With respect to this system, the Center shall ensure that for data elements related to preschool through grade 12 and postsecondary, the system meets all of the following:

- Contains a unique statewide student identifier that does not permit a student to be individually identified by users of the system, except as allowed by federal and state law.
- Contains student-level enrollment, demographic, and program participation information.
- Contains student-level information about the points at which students exit, transfer in, transfer out, drop out, or complete education programs.
- Has the capacity to communicate with higher education data systems.

For data elements related to preschool through grade 12 only, the system shall meet all of the following:

- Contains yearly test records of individual students for assessments approved by DED-OESE for accountability purposes under section 1111(b) of the Elementary and Secondary Education Act of 1965, 20 USC 6311, including information on individual students not tested, by grade and subject.
- Contains student-level transcript information, including information on courses completed and grades earned.
- Contains student-level college readiness test scores.

For data elements related to postsecondary education only:

- Contains data that provides information regarding the extent to which individual students transition successfully from secondary school to postsecondary education, including, but not limited to, all of the following: Enrollment in remedial coursework and/or Completion of 1 years' worth of college credit applicable to a degree within 2 years of enrollment.
- Contains data that provide other information determined necessary to address alignment and adequate preparation for success in postsecondary education.

Mich. Comp. Laws § 388.1694a

Use Limitations

Is sharing student data with third parties limited or prohibited?

A local or intermediate school district shall not disclose any personally identifiable information contained in a student record to a law enforcement agency, except in compliance with the Family Educational Rights and Privacy Act ("FERPA").

Mich. Comp. Laws § 180.1135

Official recruiting representatives of the armed forces of the United States or their service academies may receive pupil directory information, but shall use that information only to provide information to pupils concerning educational and career opportunities available in the armed forces or the service academies, and shall not release that information to a person who is not involved in recruiting for the armed forces or the service academies.

Mich. Comp. Laws § 380.1139

The summative assessment system shall ensure that access to individually identifiable student data is in compliance with FERPA, and except as may be provided for in an agreement with a vendor to provide assessment services, as necessary to support educator evaluations pursuant to subdivision (i), or for research or program evaluation purposes, is available only to the student; to the student's parent or legal guardian; and to a school administrator or teacher, to the extent that he or she has a legitimate educational interest.

Mich. Comp. Laws § 388.1704c

If so, are there exceptions?

Michigan does not appear to have codified any additional exceptions.

Data Minimization

Are there data retention limits?

Michigan does not appear to have

Michigan
(continued)

codified data retention limits.

Security

Is there a mandated data security program or specific security protocols?

Michigan does not appear to have codified this.

Is there required de-identification or aggregation of data?

A district or intermediate district shall comply with all applicable reporting requirements specified in state and federal law. Data provided to the center, in a form and manner prescribed by the center, shall be aggregated and disaggregated as required by state and federal law.

Mich. Comp. Laws § 388.1619

A community college shall use the P-20 longitudinal data system to inform interested Michigan high schools and the public of the aggregate academic status of its students for the previous academic year, in a manner prescribed by the Michigan Community College Association and in cooperation with the Michigan Association of Secondary School Principals.

Mich. Comp. Laws § 388.1824

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Michigan does not appear to have codified this as a requirement.

Is there a complaint process for student/parents when the law has been violated?

Michigan does not appear to have codified a complaint process to address student privacy violations

Is there a private right of action?

Not specified by statute.

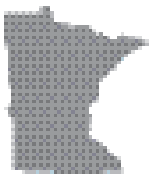
Individual Participation

Are parents/students able to opt-out of data collection or sharing?

A high school student or the parent or legal guardian of a high school pupil can submit a signed, written request to school officials of a public high school that indicates that they do not want the student's directory information to be accessible to military recruiters or representatives of service academies.

Mich. Comp. Laws § 380.1139

Minnesota



Applicable Laws

Chapter 13 of Minn. Stat. governs Governmental Data Practices

Minn. Stat. § 13.32 governs the governmental data practices regarding Educational Data

Definitions

"Educational Records"

"Educational data" means data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution which relates to a student.

Minn. Stat. § 13.32

"Covered Information" or "Student Data"

Not defined/see above.

Use Limitations

Is sharing student data with third parties limited or prohibited?

Under Minn. Stat. § 13.32, "educational data is private data on individuals and shall not be disclosed" unless one of the exceptions codified in this provision are triggered.

In any contract between a government entity subject to this chapter and any person, when the contract requires that data on individuals be made available to the contracting parties by a government entity, that data shall be administered consistent with this chapter. A contracting party shall maintain data on individuals it receives according to statutory provisions applicable to the data.

Minn. Stat. § 13.05

If so, are there exceptions?

Minn. Stat. § 13.32 codifies exceptions to the limitation on sharing educational data. These exceptions include, but are not limited to, disclosures pursuant to the provisions of the Family Educational Rights and Privacy Act ("FERPA"), pursuant to a valid court order, to volunteers who are determined to have a legitimate educational interest in the data and who are conducting activities and events sponsored by or endorsed by the educational agency or institution for students or former students and of information designated as directory information under FERPA where parents and students have been given notice and a parent or guardian has given prior written consent to the information's designation as directory information.

Data Minimization

Are there data retention limits?

Registered schools (private schools offering degree programs and out-of-state postsecondary educational institutions offering distance learning to students within Minnesota), shall maintain a permanent record for each student for 50 years from the last date of the student's attendance. Records include academic transcripts, documents, and files containing student data about academic credits earned, courses completed, grades awarded, degrees awarded, and periods of attendance.

Minn. Stat. § 136A.68

Security

Is there a mandated data security program or specific security protocols?

"The responsible authority shall:

- establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected;
- establish appropriate security safeguards for all records containing data on individuals, including procedures for ensuring that [non-public data is] only accessible to persons whose work assignment reasonably requires access to the data, and is only being accessed by those persons for purposes described in the procedure; and
- develop a policy incorporating these procedures, which may include a model policy governing access to the data," if such sharing is authorized by law.

Non-public data it must be destroyed in a way that prevents its contents from being determined.

Minn. Stat. § 13.05

Is there required de-identification or aggregation of data?

The use of summary data derived from private or confidential data on individuals under the jurisdiction of one or more responsible authorities is permitted. Summary data is public unless classified pursuant to section 13.06, another statute, or federal law. Summary data can be prepared upon the request of any person if the request is in writing and the cost of preparing the summary data is borne by the requesting person.

Minn. Stat. § 13.05

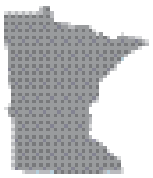
Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Each responsible authority or other appropriate authority in every government entity shall appoint or designate an employee to act as a data practices compliance official. This official is the designated employee to whom persons may direct questions or concerns regarding problems in obtaining access to data or other data practices problems.

Minn. Stat. § 13.05

Minnesota
(continued)



Is there a complaint process for student/parents when the law has been violated?

Under Minn. Stat. § 13.08, "a responsible authority or government entity which violates any provision of this chapter" is liable to a person or representative of a decedent who suffers any damage as a result of the violation and the damaged party may bring an action against the responsible party to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, a government entity is additionally liable to exemplary damages of not less than $1,000, nor more than $15,000 for each violation.

Is there a private right of action?

See above

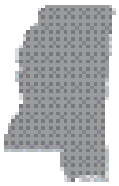
Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Before student information can be designated as directory information, which may be disclosed pursuant to FERPA, notice must be given and prior written consent granted to permit such a designation.

Minn. Stat. § 13.32

Mississippi



Applicable Laws

Title 37 of Miss. Code Ann. Governs Education

Key Provisions: Miss. Code Ann. §§ 37-15-1, et seq. and 37-154-1, 3

Definitions

"Educational Records"

Permanent Records: "The State Board of Education ["BOE"] shall prepare and provide necessary forms for keeping permanent records and cumulative folders for each pupil in the public schools, including charter schools, of the state. In the permanent record and cumulative folders, the teachers and principals shall keep information concerning the pupil's date of birth, as verified by the documentation authorized in this section, record of attendance, grades and withdrawal from the school, including the date of any expulsion from the school and a description of the student's act or behavior resulting in the expulsion. The records also shall contain information pertaining to immunization and such other information as the [BOE] may prescribe."

Miss. Code Ann. § 37-15-1

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Educational records" means those official records, files, and data directly related to a student and maintained by the school or local education agency, including, but not limited to, records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

Miss. Code Ann. § 37-135-31

"Covered Information" or "Student Data"

Not defined/see above.

Use Limitations

Is sharing student data with third parties limited or prohibited?

The school boards of all school districts have the power to delegate, privatize or otherwise enter into a contract with private entities for the operation of any and all functions of nonacademic school process, procedures and operations including data processing and student records.

Miss. Code Ann. § 37-7-301

Similarly, the State Longitudinal Data System ("SLDS") Governing Board is authorized to contract with a third party to manage and maintain the system and to insure the policies and procedures developed by the board are enforced.

Miss. Code Ann. § 37-154-3

If so, are there exceptions?

Exceptions do not appear to be codified.

Data Minimization

Are there data retention limits?

"At the point of the student's graduation or at the time when the student would normally have graduated had he not withdrawn or been expelled from school, the student's permanent record shall become a part of the permanent binder" in the central fire resistant depository, stored digitally as designated and provided by the school board of the school district, or in fire resistant storage at the school last attended by the student. The permanent binding and preservation of the inactive records shall be the duty of the superintendent of the school district who shall maintain a central depository of the records."

Miss. Code Ann. § 37-15-2

"At no time may a permanent record of a student be destroyed, but cumulative folders may be destroyed by order of the school board of the school district in not less than [five] years after the permanent record of the pupil has become inactive and has been transferred to the central depository of the district. Provided, however, that where a school district makes complete copies of inactive permanent records on [film], microfilm, or any other acceptable form of medium for storage which may be reproduced as needed, such permanent records may be destroyed after the [film] or microfilm copy has been stored in the central depository of the district."

Miss. Code Ann. § 37-15-3

Security

Is there a mandated data security program or specific security protocols?

Various agencies, including the Mississippi Department of Education, Mississippi Community College Board, and the Board of Trustees of State Institutions of Higher Learning, were charged with developing and maintaining the SLDS. The SLDS Governing Board (made up of representatives from each entity that provides data to the SLDS) will define and maintain standards for privacy, confidentiality, and security of data.

Miss. Code Ann. § 37-154-1, 3

Is there required de-identification or aggregation of data?

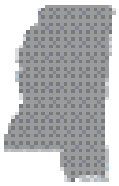
Mississippi does not appear to have codified such requirements.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Mississippi does not appear to have

Mississippi
(continued)



codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

Mississippi does not appear to have codified a complaint process for such violations.

Is there a private right of action?

Not specified by statute.

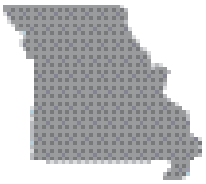
Individual Participation

Are parents/students able to opt-out of data collection or sharing?

In the context of children with disabilities, consent shall be obtained prior to the release of educational records as required under the Family Educational Rights and Privacy Act and the Individuals with Disabilities Education Act.

Miss. Code Ann. § 37-23-137

Missouri



Applicable Laws

Title XI of Mo. Rev. Stat. governs Education and Libraries

Key Provisions: Mo. Rev. Stat. § 161.096 governs Student Data Accessibility

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education(al) records" means: those official records, files, and data directly related to a student and maintained by the school or local education agency, including but not limited to records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

Mo. Rev. Stat. § 160.2000

"Covered Information" or "Student Data"

Not defined.

Use Limitations

Is sharing student data with third parties limited or prohibited?

The Missouri Department of Elementary and Secondary Education is charged with developing policies to comply with all relevant state and federal privacy laws and policies, including but not limited to the Family Educational Rights and Privacy Act ("FERPA") and other relevant privacy laws and policies. These policies are to include restricting access to personally identifiable information in the statewide longitudinal data system. Further, the Department shall not, unless otherwise provided by law and authorized by policies adopted pursuant to this section, transfer personally identifiable student data.

Mo. Rev. Stat. § 161.096

The Missouri Department of Elementary and Secondary Education shall ensure that any contracts that govern databases, assessments, or instructional supports that include student or redacted data and are outsourced to private vendors include express provisions that safeguard privacy and security, including provisions that prohibit private vendors from selling student data or from using student data in furtherance of advertising, with penalties for noncompliance, except to a local service provider for the limited purpose authorized by the school or district whose access to student data, if any, is limited to "directory information" as that term is defined in the federal regulations implementing FERPA.

Mo. Rev. Stat. § 161.096

If so, are there exceptions?

See above.

Data Minimization

Are there data retention limits?

Missouri does not appear to have codified data retention limits.

Security

Is there a mandated data security program or specific security protocols?

The Missouri Department of Elementary and Secondary Education shall develop "a detailed data security plan that includes:

- Guidelines for authorizing access to the student data system and to individual student data including guidelines for authentication of authorized access;
- Privacy compliance standards;
- Privacy and security audits;
- Breach planning, notification, and procedures;
- Data retention and disposition policies; and
- Data security policies including electronic, physical, and administrative safeguards, such as data encryption and training of employees."

Mo. Rev. Stat. § 161.096

Is there required de-identification or aggregation of data?

The Missouri Department of Elementary and Secondary Education shall produce or cause to be produced a school accountability report card. The report card is to include many data points and will permit the disclosure of data on a school-by-school basis, but the reporting shall not be personally identifiable to any student or education professional in the state.

Mo. Rev. Stat. § 160.522

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

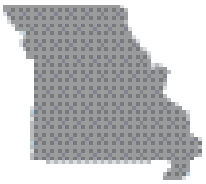
Missouri does not appear to have codified this as a requirement.

Is there a complaint process for student/parents when the law has been violated?

Each violation of any provision of any rule promulgated pursuant to Mo. Rev. Stat. § 161.096 by an organization or entity other than a state agency, a school board, or an institution shall be punishable by civil penalties (of increasing value with subsequent violations by the same organization or entity). However, this right to commence civil action appears to be intended for the attorney general.

Mo. Rev. Stat. § 161.096

Missouri
(continued)



Is there a private right of action?

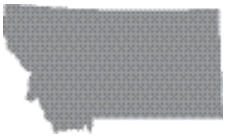
See above.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Missouri does not appear to have codified an ability to opt-out.

Montana



Applicable Laws

10.55.909 STUDENT RECORDS (Administrative Rules of Montana);

Montana Code Ann. (2015): 20-1-213(5); 20-1-212; 20-25-511; 20-25-515; 20-7-104; 41-5-1707

Definitions

"Educational Records"

According to 10.55.909 there is a permanent record that includes the name and address of the student; his/ her parent or guardian; birth date; academic work completed; level of achievement (grades, standardized achievement tests); immunization records as per 20-5-406, MCA; attendance data; and the statewide student identifier assigned by the Office of Public Instruction. There are also non-permanent student records which are records retained in a central file maintained by the school containing a student's cumulative educational records, which are not retained as a student's permanent record (aforementioned data).

"Covered Information" or "Student Data"

Not defined.

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes. In addition to the data privacy protections in subsection (1)(b), the superintendent of public instruction may provide personally identifiable information gathered, maintained, and distributed pursuant to subsection (7) and any other personally identifiable data only to the office of public instruction, the school district where the student is or has been enrolled, the parent, and the student. The superintendent of public instruction may not share, sell, or otherwise release personally identifiable information to any for-profit business, nonprofit organization, public-private partnership, governmental unit, or other entity unless the student's parent has provided written consent specifying the data to be released, the reason for the release, and the recipient to whom the data may be released.

20-7-104(9)

The office of public instruction's statewide data system must, at a minimum . . . display a publicly available educational data profile for each school district that protects each student's education records in compliance with the Family Educational Rights and Privacy Act of 1974 ("FERPA").

20-7-104(1)(b)

For university or college students, the school shall release a student's academic record only when requested by the student or by a subpoena issued by a court or tribunal of competent jurisdiction. A student's written permission must be obtained before the university or college may release any other kind of record unless such record shall have been subpoenaed by.

20-25-515

If so, are there exceptions?

Montana school districts may release education records to assessment officers, who are responsible for ensuring that officials and authorities to whom that information is disclosed certify in writing to the school district that is releasing the education records that the education records or information from the education records will not be disclosed to any other party without the prior written consent of the parent of the student.

41-5-1707

A local educational agency or accredited school may release student information to the juvenile justice system to assist the system's ability to effectively serve, prior to adjudication, the student whose records are released under provisions of FERPA. The official to whom the records are disclosed shall certify in writing to the sending official that the information will not, except as provided by law, be disclosed to any other party without prior written consent of the parent of the student.

20-1-213(5)

Data Minimization

Are there data retention limits?

After the retention period in 2-6-1202 is complete and records are not needed any more, each student's permanent file (as defined by the board of public education) must be kept in a secure location permanently. Other student records must be maintained and destroyed as provided in the retention schedules.

20-1-212

Security

Is there a mandated data security program or specific security protocols?

Montana has adopted Generally Accepted Record Keeping Principles from ARMA for local government electronic systems and recommends the adoption of the same.

Is there required de-identification or aggregation of data?

Not specified by statue.

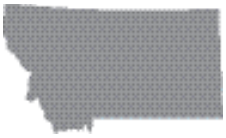
Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

ARMA requires an executive of some sort- but these are recommendations for local governments to adopt. There is nothing else that speaks to this.

Is there a complaint process for student/parents when the law has

Montana
(continued)



been violated?

Montana does not appear to have codified a complaint process in regards to student privacy violations.

Is there a private right of action?

Montana does not appear to have codified a private right of action in regards to student privacy violations.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Montana does not appear to have codified an ability to opt-out of data collection or sharing.

Nebraska

Applicable Laws

Chapter 79 of Neb. Rev. Stat. governs Schools

Key Provisions: Neb. Rev. Stat. § 7-2,104 (governing access to school files or records)

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education records" or "educational records" means those official records, files, and data directly related to a student and maintained by the school or local education agency, including, but not limited to, records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

Neb. Rev. Stat. § 79-2201

"Covered Information" or "Student Data"

Not defined.

Use Limitations

Is sharing student data with third parties limited or prohibited?

The State Board of Education shall enter into memoranda of understanding on or before September 1, 2010, with the Board of Regents of the University of Nebraska, the Board of Trustees of the Nebraska State Colleges, and the board of governors of each community college area to adopt a policy to share student data. At a minimum, the policy shall ensure that the exchange of information is conducted in conformance with the requirements of the Family Educational Rights and Privacy Act ("FERPA").

Neb. Rev. Stat. § 79-776

Any student in any public school or his or her parents, guardians, teachers, counselors, or school administrators shall have access to the school's files or records maintained concerning such student, including the right to inspect, review, and obtain copies of such files or records. No other person shall have access to such files or records except (a) when a parent, guardian, or student of majority age provides written consent or (b) as provided in subsection (3) of this section. The contents of such files or records shall not be divulged in any manner to any unauthorized person.

Neb. Rev. Stat. § 79-2,104

If so, are there exceptions?

Neb. Rev. Stat. § 79-2,104(3) enables auditing officials of the United States and Nebraska, as well as state educational authorities, to access student or other records to audit and evaluate federal- or state-supported education programs or in connection with the enforcement of legal requirements related to such programs. Additionally, student records may be disclosed in a manner consistent with FERPA and the regulations adopted thereunder.

Data Minimization

Are there data retention limits?

A school's files or records regarding a student shall be maintained so as to separate academic and disciplinary matters, and all disciplinary material shall be removed and destroyed after a student's continuous absence from the school for a period of three years.

Neb. Rev. Stat. § 79-2,104

Personally identifiable data shall be destroyed when no longer needed for audit, evaluation, or enforcement of legal requirements to be conducted by auditing officials of the United States and Nebraska or other state educational authorities.

Neb. Rev. Stat. § 79-2,104

Security

Is there a mandated data security program or specific security protocols?

Nebraska does not appear to have codified a mandate for a data security program or specific security protocols.

Is there required de-identification or aggregation of data?

The State Board of Education shall implement a statewide system for tracking individual student achievement, using the student identifier system of the State Department of Education, that can be aggregated to track student progress by demographic characteristics, including, but not limited to, race, poverty, high mobility, attendance, and limited English proficiency, on available measures of student achievement which include, but need not be limited to, national assessment instruments, and state assessment instruments, among other indicators.

Neb. Rev. Stat. § 79-760.05

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Nebraska does not appear to have codified such a requirement.

Is there a complaint process for student/parents when the law has been violated?

Nebraska does not appear to have codified such a complaint process.

Is there a private right of action?

N/A

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Nebraska does not appear to have codified an opt-out.

Nevada

Applicable Laws

Title 34 of Nev. Rev. Stat. governs Education

Key Provisions: Nev. Rev. Stat. § 392.029; Nev. Rev. Stat. SB 463 §§ 1.5, et seq. (note, these provisions have been approved by the Governor, effective July 1, 2015, but not yet codified as they are subject to change from the reviser of the Nevada Legislative Bureau)

Definitions

"Educational Records"

"Education records" has the meaning ascribed to the term in the Family Educational Rights and Privacy Act ("FERPA").

Nev. Rev. Stat. § 392.029

"Covered Information" or "Student Data"

Not defined.

Use Limitations

Is sharing student data with third parties limited or prohibited?

Except as otherwise provided in FERPA, a public school shall not release the education records of a pupil to a person, agency, or organization without the written consent of the parent or legal guardian of the pupil.

Nev. Rev. Stat. § 392.029

A school service provider, defined as a website, online service, or mobile application that collected personally identifiable information concerning a pupil, is used primarily for educational purposes, and is designed and marketed for use in public schools, is barred from using personally identifiable information to engage in targeted advertising, from selling it, from using it to improperly create a profile of the pupil, from using it in a manner inconsistent with any contract governing the activities of the school service provider for the school service, or from knowingly retaining the information beyond the period authorized by the contract without consent.

Nev. Rev. Stat. SB 463 § 6

If so, are there exceptions?

Nev. Rev. Stat. SB 463 § 6 enumerates exceptions to the limitations.

Data Minimization

Are there data retention limits?

A school service provider shall delete any personally identifiable information concerning a pupil that is collected

or maintained by the school service provider and that is under the control of the school service provider within a reasonable time not to exceed 30 days after receiving a request from the board of trustees of the school district in which the school that the pupil attends is located, the governing body of the charter school that the pupil attends or the governing body of the university school for profoundly gifted pupils that the pupil attends, as applicable. The board of trustees or the governing body, as applicable, must have a policy which allows a pupil who is at least 18 years of age or the parent or legal guardian of any pupil to review such information and request that such information about the pupil be deleted. The school service provider shall delete such information upon the request of the parent or legal guardian of a pupil

if no such policy exists.

Nev. Rev. Stat. SB 463 § 6

Security

Is there a mandated data security program or specific security protocols?

A school service provider shall establish and carry out a detailed plan for the security of any data concerning pupils that is collected or maintained by the school service provider. The plan must include, without limitation:

- Procedures for protecting the security, privacy, confidentiality and integrity of personally identifiable information concerning a pupil; and
- Appropriate administrative, technological and physical safeguards to ensure the security of data concerning pupils.

Nev. Rev. Stat. SB 463 § 7

Is there required de-identification or aggregation of data?

AA school service provider may use and disclose information derived from personally identifiable information concerning a pupil to demonstrate the effectiveness of the products or services of the school service provider, including, without limitation, for use in advertising or marketing regarding the school service so long as the information is aggregated or is presented in a manner which does not disclose the identity of the pupil about whom the information relates.

Nev. Rev. Stat. SB 463 § 8.3

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

A CPO requirement is not apparent.

Is there a complaint process for student/parents when the law has been violated?

There does not appear to be a codified complaint process for student privacy violations.

Is there a private right of action?

A civil penalty for violation of Nev. Rev. Stat. SB 463 § 6 is available to the Attorney General to bring in the name of the State of Nevada.

Individual Participation

Nevada
(continued)

Are parents/students able to opt-out of data collection or sharing?

Parents and eligible students shall have the right to consent to the sharing of education records consistent to those rights enumerated in FERPA.

Nev. Rev. Stat. §§ 392.029; 386.655

New Hampshire

Applicable Laws

Title XV of N.H. Rev. Stat. Ann. Governs Education

Key Provisions: N.H. Rev. Stat. Ann. § 189;65, et seq.

Definitions

"Educational Records"

See below.

"Covered Information" or "Student Data"

"Student personally-identifiable data" means":

The student's name; the name of the student's parents or other family members; the address of the student or student's family; indirect identifiers, including the student's date and place of birth, SSN, email, social media, or other electronic address, telephone number, credit card account number, insurance account number, and financial services account number; and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

N.H. Rev. Stat. Ann. § 189:65

"Covered information" means personally identifiable information or materials, in any media or format that meets any of the following:

- Is created or provided by a student, or the student's parent or legal guardian, to an operator in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for K-12 school purposes.
- Is created or provided by an employee or agent of the K-12 school, school district, local education agency, or county office of education, to an operator.
- Is gathered by an operator through the operation of a site, service, or application described in subparagraph (a) and is descriptive of a student or otherwise identifies a student, including, but not limited to, [information listed in § 189:65, as well as], information in the student's educational record or email, unique pupil identifier, other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical or health records, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, other student identifiers, search activity, photos, voice recordings, or geo-location.

N.H. Rev. Stat. Ann. § 189:68-a

Use Limitations

Is sharing student data with third parties limited or prohibited?

Student personally-identifiable data Student personally-identifiable data shall be considered confidential and privileged and shall not be disclosed, directly or indirectly, as a result of administrative or judicial proceedings.

N.H. Rev. Stat. Ann. § 189:67

Neither a school nor the department shall disclose or permit the disclosure of student or teacher personally-identifiable data, the unique pupil identifier, or any other data listed in § 189:68 to any testing entity performing test-data analysis. The testing entity may perform test analysis but shall not connect such data to other student data.

N.H. Rev. Stat. Ann. § 189:67

An operator of a website, online service, or application used primarily for K-12 school purposes ("an operator") shall not knowingly engage in targeted advertising based upon information acquired through the operator's services, use the information to improperly amass a profile of a student, sell or otherwise make available a student's information, or disclose protected information unless the disclosure is made pursuant to judicial process.

N.H. Rev. Stat. Ann. § 189:68-a

If so, are there exceptions?

A school or the department may disclose a student's birth date and either the student's name or unique pupil identifier to a testing entity for the sole purpose of identifying the test taker. This data is to be destroyed as soon as the testing entity has completed the verification of the test taker, and the information is not to be disclosed to other third parties for any other purpose.

N.H. Rev. Stat. Ann. § 189:67

Local education agencies which maintain education records may provide information designated as directory information consistent with the Family Educational Rights and Privacy Act ("FERPA"), which may include name and address of a student, athletes weight and height, date and place of birth, and field of study, among other items.

N.H. Rev. Stat. Ann. § 189:1-e

Data Minimization

Are there data retention limits?

An operator is directed to delete a student's covered information if the school or district requests deletion of data under the control of the school or district.

N.H. Rev. Stat. Ann. § 189:69-a

New Hampshire
(continued)

Security

Is there a mandated data security program or specific security protocols?

The New Hampshire Department of Education is tasked with developing a detailed data security plan to include: (a) Privacy compliance standards; (b) Privacy and security audits; (c) Breach planning, notification, and procedures; and (d) Data retention and disposition policies.

N.H. Rev. Stat. Ann. § 189:65

An operator is charged with implementing and maintaining reasonable security procedures and practices appropriate to the nature of the covered information, and protecting that information from unauthorized access, destruction, use modification, or disclosure.

N.H. Rev. Stat. Ann. § 189:68-a

Is there required de-identification or aggregation of data?

An operator may use de-identified student covered information within the operator's [service] or other [services] owned by the operator to improve educational products and to demonstrate the effectiveness of the operator's services, including in its marketing. An operator may further share aggregated de-identified student covered information for the development and improvement of educational sites, services, or applications.

N.H. Rev. Stat. Ann. § 189:68-a

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

New Hampshire does not appear to have codified such a requirement.

Is there a complaint process for student/parents when the law has been violated?

A student or parent has the right to file a complaint with the Family Policy Compliance Office in the United States Department of Education concerning alleged failures to comply with the requirements of FERPA.

N.H. Rev. Stat. Ann. § 189:66

Is there a private right of action?

See above.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

The Department of Education shall make publicly available students' and parents' rights under FERPA and applicable state law, including the right to provide written consent before the school discloses student personally identifiable data from the student's education records, provided in applicable state and federal law.

N.H. Rev. Stat. Ann. § 189:66

New Jersey

Applicable Laws

Title 18A of N.J. Stat. Ann. governs Education

N.J. Admin. Code § 6A:32-7.1, et seq. (governing Student Records)

Definitions

"Educational Records"

The State Board of Education shall provide by regulation for the creation, maintenance, and retention of pupil records and for the security thereof and access thereto to provide general protection for the right of the pupil to be supplied with necessary information about herself or himself, the right of the parent or guardian and the adult pupil to be supplied with full information about the pupil, except as may be inconsistent with reasonable protection of the persons involved, the right of both pupil and parent or guardian to reasonable privacy as against other persons, and the opportunity for the public schools to have the data necessary to provide a thorough and efficient educational system for all pupils.

N.J. Stat. Ann. § 18A:36-19

Student Records: Each district board of education shall compile and maintain student records and regulate access, disclosure, or communication of information contained in educational records in a manner that assures the security of such records. Student records shall contain only such information as is relevant to the education of the student and is objectively based on the personal observations or knowledge of the certified school personnel who originate(s) the record.

N.J. Admin. Code § 6A:32-7.1

Mandated student records shall include the following:

- The student's name, address, telephone number, date of birth, name of parent(s), gender, standardized assessment results, grades, attendance, classes attended, grade level completed, year completed, and years of attendance;
- Record of daily attendance;
- Descriptions of student progress according to the student evaluation system used in the school district;
- History and status of physical health compiled in accordance with State regulations, including results of any physical examinations given by qualified school district employees and immunizations;
- Records pursuant to rules and regulations regarding the education of students with disabilities; and
- All other records required by N.J. Admin. Code § 6A

N.J. Admin. Code § 6A:32-7.3

"Covered Information" or "Student Data"

"Pupil directory information" means a pupil's name and address. N.J. Stat. Ann. § 18A:54-20.3

Use Limitations

Is sharing student data with third parties limited or prohibited?

Only authorized organizations, agencies or persons, as defined, shall have access to student records, including student health records. Individuals shall adhere to the Family Educational Rights and Privacy Act ("FERPA").

N.J. Admin. Code § 6A:32-7.5

The board of education of each school district and the board of trustees of each charter school that establishes an internet web site shall not disclose on that web site any personally identifiable information about a student without receiving prior written consent from the student's parent or guardian on a form developed by the Department of Education.

N.J. Stat. Ann. § 18A:36-35

If so, are there exceptions?

In addition to the declaration that FERPA applies, school personnel may disclose information contained in student health records to students or adults in connection with an emergency.

N.J. Admin. Code § 6A:32- 7.5

Data Minimization

Are there data retention limits?

Mandated student records required as part of programs established through State-administered entitlement or discretionary funds from the U.S. Department of Education shall be maintained for a period of five years after graduation, termination from the school district, or age 23, whichever is longer, and shall be disposed of in accordance with the New Jersey Destruction of Public Records Law (codified at N.J. Stat. Ann. §§ 47:3–15 et seq.).

N.J. Admin. Code § 6A:32-7.4

The New Jersey public school district of last enrollment, graduation, or permanent departure of the student from the school district shall keep for 100 years a mandated record of a student's name, date of birth, name of parents, gender, health history and immunization, standardized assessment results, grades, attendance, classes attended, grade level completed, year completed, and years of attendance.

N.J. Admin. Code § 6A:32-7.8

Upon the annual review of student records, the chief school administrator or his or her designee shall cause data no longer descriptive of the student or educational program to be deleted from the records.

N.J. Admin. Code § 6A:32-7.1

New Jersey
(continued)

Security

Is there a mandated data security program or specific security protocols?

Each district school board is charged with establishing written policies and procedures that assure the security of student records.

N.J. Admin. Code § 6A:32-7.1

Is there required de-identification or aggregation of data?

Where bone fide researchers are using student records, they must confirm in writing that the records will be used under strict conditions of anonymity and confidentiality prior to the release of those records.

N.J. Admin. Code § 6A:32-7.5

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

The chief school administrator or his or her designee shall be responsible for the security of student records maintained in the school district and shall devise procedures for assuring that access to such records is limited to authorized persons.

N.J. Admin. Code § 6A:32-7.4

Is there a complaint process for student/parents when the law has been violated?

Student records are subject to challenge by parents and adult students on grounds of inaccuracy, irrelevancy, impermissive disclosure, inclusion of improper information or denial of access to organizations, agencies and persons.

N.J. Admin. Code § 6A:32-7.7

Is there a private right of action?

See above.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Each district school board is charged with establishing written policies and procedures that provide the parent or adult student a 10-day period to submit to the chief school administrator a written statement prohibiting the institution from including any or all types of information about the student in any student information directory before allowing access to such directory and school facilities to educational, occupational, and military recruiters.

N.J. Admin. Code § 6A:32- 7.1

New Mexico

Applicable Laws

Chapters 22 and 22A of N.M. Stat. Ann. govern Public Schools

N.M. Code R. § 6.29.1.9(E) governs Records and Reports

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "education records" means records, files and data that are directly related to a student and maintained by a school or local education agency,

including records encompassing all the material kept in a student's cumulative folder such as general identifying

data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

N.M. Stat. Ann. § 11-8B-1

Use Limitations

Is sharing student data with third parties limited or prohibited?

No public or private post-secondary educational institution, including its agents, its employees, its student or alumni organizations or its affiliates, shall sell, give or otherwise transfer to any card issuer, for the purpose of distributing or marketing credit cards, the name, address, social security number, date of birth, telephone number or other contact or personal identifying information of an undergraduate student at the post-secondary educational institution.

N.M. Stat. Ann. § 21-1-45

Each district and charter school shall maintain and treat all personally identifiable educational records in accordance with the Family Educational Rights and Privacy Act ("FERPA") and its implementing regulations and the Inspection of Public Records Act, codified at N.M. Stat. Ann. § 14-2-1 – 12. N.M. Code R. § 6.29.1.9(E)

If so, are there exceptions?

Other than those exceptions found in FERPA, New Mexico does not appear to have codified additional exceptions.

Data Minimization

Are there data retention limits?

New Mexico does not appear to have codified such limits.

Security

Is there a mandated data security program or specific security protocols?

The data system council, comprised of data system partners who will be inputting information into the data system, is charged with assisting the educational agencies whose data is to be included in the data system to develop interagency agreements in

order to assure the security of the data system and to ensure the privacy of any person whose personally identifiable information is contained in the data system.

N.M. Stat. Ann. § 21-1-11

Is there required de-identification or aggregation of data?

Data system partners, in consultation with school districts, charter schools and public post-secondary educational institutions, may collect and distribute aggregate data about students or educators or data about an individual student or educator without personally identifiable information.

N.M. Stat. Ann. § 21-1-11

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

While New Mexico has not codified a

requirement for a CPO, it has created a "data system council" to oversee the longitudinal student-level and educator

data system.

N.M. Stat. Ann. § 21-1-11

Is there a complaint process for student/parents when the law has been violated?

A parent or eligible student may bring a complaint with the U.S. Department of Education concerning non- compliance with FERPA.

N.M. Code R. § 6.29.1.7(AT)

Is there a private right of action?

Yes. A person whose contact information was sold, given or transferred to a card issuer in violation of N.M. Stat. Ann. § 21-1-45, or the attorney general, may bring a civil action and seek a civil penalty in an amount not to exceed $10,000 for each violation plus costs of the action and reasonable attorney fees.

N.M. Stat. Ann. § 21-1-45

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

FERPA grants the right to consent or refuse to consent to disclosures of personally identifiable information in the student's records (except for those records that FERPA authorizes for disclosure without consent).

N.M. Code R. § 6.29.1.7(AT)

New York

Applicable Laws

New York State Education Law § 2-d ("Section 2-d") [created by New York Assembly Bill 8556 / New York Senate Bill 6356, signed into law 3/31/2014]

New York State Education Law § 2-c ("Section 2-c") [created by New York Assembly Bill 8556 / New York Senate Bill 6356, signed into law 3/31/2014]

Definitions

"Educational Records"

[Section 2-d]: Refers to "student records" but does not define what those records include.

"Covered Information" or "Student Data"

[Section 2-c]: "Student Information" means personally identifiable information and biometric records as defined in Section 99.3 of Title 34 of the CFR implementing the Family Educational Rights and Privacy Act ("FERPA").

[Section 2-d]: "Student Data" means personally identifiable information from student records of an educational agency.

Adopts the definition of "Personally Identifiable Information" in Section 99.3 of Title 34 of the CFR implementing FERPA.

Use Limitations

Is sharing student data with third parties limited or prohibited?

[Section 2-c]:

Allows an educational agency to opt-out of providing personally identifiable information of a student to a "shared learning infrastructure service provider" ("SLISP") or data dashboard operator for the purpose of creating data dashboards. The educational agency has the right to request that any personally identifiable information of its students not be shared with or provided to a SLISP or data dashboard operator at any time. This request must be made directly to the New York State Education Department ("NYSED").

Prohibits the Commissioner of Education and NYSED from sharing any student information to a SLISP.

[Section 2-d]:

Data Security and Privacy Plan: Each third party contractor with which an education agency contracts must clearly include a data security and privacy plan that outlines how all state, federal, and local data security and privacy contract requirements will be implemented over the life of the contract, consistent with the educational agency's policy on data security and privacy. Such plan shall include, but shall not be limited to, a signed copy of the parent's bill of rights for data privacy and security, and a requirement that any officers or employees of the third party contractor and its assignees who have access to student data or teacher or principal data have received or will receive training on the federal and state law governing confidentiality of such data prior to receiving access.

Limits on Third Party Contractors: Each third party contractor receiving student data or teacher/principal data shall:

Limit internal access to education records to those individuals that are determined to have legitimate educational interests;

Not use the education records for any other purposes than those explicitly authorized in its contract;

Except for authorized representatives of the third party contractor to the extent they are carrying out the contract, not disclose any personally identifiable information ("PII") to any other party: (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 notice of the disclosure to the department, 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;

Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody; and

Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the united states department of health and human services in guidance issued under section 13402(h)(2) of public law 111-5.

Breach Notification: Third party contractors are required to notify the educational agency in the event of a breach of student and/or teacher/ principal data.

If so, are there exceptions?

[Section 2-d]: A third party contractor may disclose PII of a student or teacher/ principal if: (1) the transfer is with an authorized representative of the third party; or (2) the third party has the prior written consent of the parent or eligible student; or (3) disclosure is required by law and the third party provides prior notice to the educational agency before disclosure, provided it is permitted by law.

Data Minimization

Are there limits on how long data can/should be retained?

[Section 2-d]: The language of the law does not contain specific provisions on the length of time data can/ should be retained, but forthcoming implementing regulations may.

New York (continued)

[Section 2-c]: In the event an educational agency makes a request to the NYSED that any personally identifiable information not be shared or provided to a Shared Learning Infrastructure Service Provider ("SLISP") [an entity that collects, stores, organizes, or aggregates student data for the purposes of providing student information to a data dashboard operator] or data dashboard operator [electronic data system or hosted software application designed to utilize data and information collected by a SLISP and provides access to customized student information for purposes of student learning], any PII provided must be deleted or destroyed in a secure manner.

Security

Is there a mandated data security program or specific security protocols?

[Section 2-d]: While implementing regulations have not been developed as of November 2015, the law requires the Chief Privacy Officer to develop standards for data security and privacy policies that shall include, but not be limited to:

(1) data privacy protections, including criteria for determining whether a proposed use of personally identifiable information would benefit students and educational agencies, and processes to ensure that personally identifiable information is not included in public reports or other public documents;

(2) data security protections, including data systems monitoring, data encryption, incident response plans, limitations on access to personally identifiable information, safeguards to ensure personally identifiable information is not accessed by unauthorized persons when transmitted over communication networks, and destruction of personally identifiable information when no longer needed; and

(3) application of all such restrictions, requirements and safeguards to third-party contractors.

Following promulgation of implementing regulations, each educational agency shall ensure that it has a policy on data security and privacy in place that is consistent with applicable state and federal laws which shall be published on the educational agency's website. Notice of such policy shall be provided to all officers and employees of the educational agency. Breach Notification: Additionally, third party contractors are required to notify the educational agency in the event of a breach of student and/or teacher/principal data.

Is there required de-identification or aggregation of data?

[Section 2-d]: The language of the law does not contain specific provisions for the de-identification or aggregation of student data or teacher/principal data, but forthcoming implementing regulations may.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

[Section 2-d]: Requires the Commissioner of Education to appoint a Chief Privacy Officer ("CPO") within the Education Department for a term of 3 years, which may be renewed for additional 3-year terms.

The functions of the CPO include:

- Promoting the implementation of sound information practices for privacy and security of student data and teacher/principal data;
- Assisting the Commissioner in handling instances of data breaches of student data and/or teacher/principal data;
- Assisting New York educational agencies with establishing minimum standards and best practices for data privacy and security;
- Creating a procedure for requests for information pertaining to student data by parents, students, teachers, superintendents, school board members, principals, among others;
- Assisting the Commissioner in establishing a protocol for the submission of complaints of possible breaches of student data or teacher/principal data;
- Making recommendations as needed regarding privacy and the security of student data on behalf of the department to the governor, the speaker of the assembly, the temporary president of the senate, and the chairs of the senate and assembly education committees; and
- Issuing an annual report on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaint submitted.

Is there a complaint process for student/parents when the law has been violated?

[Section 2-d]: Parents have the right to file complaints with an educational agency about possible breaches of student data by that educational agency's third party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail. nysed.gov.

Parents also have the right inspect and review their child's educational record including any student data stored or maintained by an educational agency. The law states that the NYSED shall develop policies for school districts

New York
(continued)

that: (1) provide for annual notification to parents of their right to request student data; (2) ensure security when providing student data to parents, including that only authorized individuals receive such data; and (3) specify a reasonable amount of time in which school districts should respond to such requests.

Is there a private right of action?

No private right of action for any of the laws/bills listed.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

[Section 2-d]: Parents are not able to opt-out of data collection, but they do have the right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent (including but not limited to disclosure under specified conditions to: (i) school officials within the school or school district with legitimate educational interests; (ii) officials of another school for purposes of enrollment or transfer; (iii) third party contractors providing services to, or performing functions for an educational agency; (iv) authorized representatives of the U.S. Comptroller General, the U.S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as NYSED; (v) organizations conducting studies for or on behalf of educational agencies) and (vi) the public where the school or school district has designated certain student data as "directory information" under FERPA.

[Section 2-c]: An educational agency may opt out of providing personally identifiable information to a SLISP or data dashboard operator for the purpose of creating data dashboards.

North Carolina

Applicable Laws

Chapter 115C of N.C. Gen. Stat. governs Elementary and Secondary Education

Chapter 116E-1 of N.C. Gen. Stat. governs the Education Longitudinal Data System

Key Provisions: N.C. Gen. Stat. §§ 115C-402, et seq.

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education(al) records" means: those official records, files, and data directly related to a student and maintained by the school or local education agency, including but not limited to records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

N.C. Gen. Stat. § 115C-407.5

Official Record of a Student: The official record shall contain, as a minimum, adequate identification data including date of birth, attendance data, grading and promotion data, and such other factual information as may be deemed appropriate by the local board of education having jurisdiction over the school wherein the record is maintained.

N.C. Gen. Stat. § 115C-402

"Covered Information" or "Student Data"

Personally identifiable student data—student data that:

- Includes, but is not limited to, the following: Student name; Name of the student's parent or other family members; Address of the student or student's family; Personal identifier, such as the student's SSN or unique student identifier.
- Other indirect identifiers, such as the student's DOB of birth, place of birth, and mother's maiden name.
- Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.
- Information requested by a person who the Department of Public Instruction or local school administrative unit reasonably believes knows the identity of the student to whom the education record relates.
- Does not include directory information that a local board of education has provided parents with notice of and an opportunity to opt out of disclosure of that information, as provided under the Family Educational Rights and Privacy Act ("FERPA"), unless a parent has elected to opt out of disclosure of the directory information.

N.C. Gen. Stat. § 115C-402.5

"Personally identifiable information" means any information directly related to a student, including the student's name, birthdate, address, social security number, individual purchasing behavior or preferences, parents' names, telephone number, or any other information or identification number that would provide information about a specific student.

N.C. Gen. Stat. § 115C-401.1

Use Limitations

Is sharing student data with third parties limited or prohibited?

A person who has entered into a contract with a local board of education or its designee may not sell any personally identifiable information obtained from a student as a result of the person's performance under the contract (unless the person obtains prior written consent from the student's parent or guardian).

N.C. Gen. Stat. § 115C-401.1

The official record of each student is not a public record and shall not be subject to inspection and examination.

N.C. Gen. Stat. § 115C-402

The N.C. Board of Education is charged with overseeing the routine and ongoing compliance with FERPA and other relevant privacy law and policies.

N.C. Gen. Stat. § 116E-4

If so, are there exceptions?

North Carolina does not appear to have codified specific exceptions.

Data Minimization

Are there data retention limits?

The official record of each student enrolled in North Carolina public schools shall be permanently maintained in the files of the appropriate school after the student graduates, or should have graduated, from high school unless the local board determines that such files may be filed in the central office or other location designated by the local board for that purpose.

N.C. Gen. Stat. § 115C-402

Security

Is there a mandated data security program or specific security protocols?

The N.C. Board of Education is charged with developing a detailed data security plan for the student data system that includes all of the following:

- Guidelines for authorizing access

North Carolina (continued)

to the student data system and to individual student data, including guidelines for authentication of authorized access.

- Privacy compliance standards.
- Privacy and security audits.
- Breach planning, notification, and procedures.
- Data retention and disposition policies.
- Data security policies, including electronic, physical, and administrative safeguards such as data encryption and training of employees.

N.C. Gen. Stat. § 115C-402.5

Is there required de-identification or aggregation of data?

"Aggregate student data" and "de-identified student data" are defined at N.C. Gen. Stat. § 115C-402.5

The N.C. Board of Education shall ensure that any contracts for the student data system that include de-identified student data or personally identifiable student data and are outsourced to private contractors include express provisions that safeguard privacy and security and include penalties for noncompliance.

N.C. Gen. Stat. § 115C-402.5

Only de-identified data shall be used in the analysis, research, and reporting conducted by the North Carolina Longitudinal Data System. And the System shall only use aggregate data in the release of data in reports and in response to data requests.

N.C. Gen. Stat. § 116E-5

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

North Carolina does not appear to have codified a requirement for a CPO.

Is there a complaint process for student/parents when the law has been violated?

Parents and eligible students may file a complaint with the U.S. Department of Education concerning alleged failures to comply with the Family Educational Rights and Privacy Act.

N.C. Gen. Stat. § 115C-402.15

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Local boards of education shall annually provide parents, by a method reasonably designed to provide actual notice, information on parental rights under state and federal law with regards to student records and opt-out opportunities for disclosure of directory information as provided under FERPA, and notice and opt- out opportunities for surveys covered by the Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h.

N.C. Gen. Stat. § 115C-402.15

North Dakota

Applicable Laws

Title 15.1 of N.D. Cent. Code governs Elementary and Secondary Education

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Educational records" means official records, files, and data directly related to a student and maintained by the student's school or school district, including records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

N.D. Cent. Code § 15.1-04.1-01

"Covered Information" or "Student Data"

Not defined.

Use Limitations

Is sharing student data with third parties limited or prohibited?

The board of each school district shall adopt a policy regarding the protection of student data. The policy must require that permission be obtained from the board before any student data is shared with an individual who is not a school district employee or shared with any other entity. This provision does not apply to the sharing of data with a student's parent or to the sharing of data, if required by law.

N.D. Cent. Code § 15.1-07-25.3

If so, are there exceptions?

Subject to the limitations on the disclosure of directory information under the Family Educational Rights and Privacy Act ("FERPA"), each high school shall provide to the North Dakota university system a list of all students enrolled in grades ten and eleven as of April fifteenth of each year, together with the students' addresses and telephone numbers. The North Dakota university system shall disclose this information to each institution under the control of the state board of higher education and to each nonpublic university and college in this state.

N.D. Cent. Code § 15.1-07-25.1

Data Minimization

Are there data retention limits?

The statewide longitudinal data system committee shall establish policies and adopt rules addressing access to and the collection, storage, and sharing of information and the systems necessary to perform those functions, subject to applicable federal and state privacy laws and interagency agreements and restrictions relating to confidential information required to conform to applicable federal and state privacy laws.

N.D. Cent. Code § 54-59-34

Records regarding a student obtained by a school under section 15.1-19-14, section 27-20-51, or section 27-20-52 (each addressing juvenile or school law enforcement) must be destroyed when the student reaches the age of eighteen or no longer attends the school, whichever occurs later.

N.D. Cent. Code § 15.1-19-15

Security

Is there a mandated data security program or specific security protocols?

The statewide longitudinal data system committee in consultation with the information technology department shall:

- Establish the terms and conditions under which a person may be authorized to access data through the statewide longitudinal data system;
- Direct that all statewide longitudinal data system administrators implement approved data protection practices to ensure the security of electronic and physical data, provided that the practices include requirements for encryption and staff training;
- Provide for biennial privacy and security audits of the statewide longitudinal data system;
- Establish protocols, including procedures, for the notification of students and parents in the event of a data breach involving the statewide longitudinal data system;
- Require that data retention and disposition by the statewide longitudinal data system be governed by the same policies as those instituted for the information technology department; and
- Require the provision of annual training regarding data protection to any individuals who have access to the statewide longitudinal data system, including school district employees, employees of the North Dakota university system office and institutions under the control of the state board of higher education, and elected or appointed state or local governmental officials.

N.C. Cent. Code § 54-59-34

Is there required de-identification or aggregation of data?

North Dakota does not appear to have codified such a requirement.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

North Dakota does not appear to have codified such a requirement.

North Dakota
(continued)

Is there a complaint process for student/parents when the law has been violated?

North Dakota does not appear to have codified a complaint process with respect to student privacy issues.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

For student data not shared with a parent or legal guardian or shared as required by law, the board of each school district is charge with instituting a policy to obtain consent before sharing student data with an entity or individual who is not a school district employee.

N.D. Cent. Code § 15.1-07- 25.3

Ohio

Applicable Laws

Ohio Administrative Code §§ 3301-2; 3301-2-03; 3301-2-05; 3301-2-12; 3301-2-16; 3301-2-17

Ohio Revised Code §§ 149.011; 149.34; 149.43; 1347.15; 1349.19; 3301.0714; 3301.0716; 3301.94; 3301.133; 3301.941; 3301.947; 3301.948; 3310.11; 3310.42; 3310.63; 3313.978; 33178.20; 3319.321

Definitions

"Educational Records"

Used in statute (Ohio Revised Code § 3301.94), but undefined.

State "records" are generally defined as "any document, device, or item, regardless of physical form or characteristic, including an electronic record as defined in section 1306.01 of the Revised Code, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office."

Ohio Revised Code § 149.011

Under the Ohio Breach Notification statute (Ohio Revised Code § 1349.19) "Record" means any information that is stored in an electronic medium and is retrievable in perceivable form. "Record" does not include any publicly available directory containing information an individual voluntarily has consented to have publicly disseminated or listed, such as name, address, or telephone number.

Ohio Revised Code §§ 1349-19

"Covered Information" or "Student Data"

Used in statute (Ohio Revised Code § 3301.94) but undefined. "Student Data" likely includes aggregated data on the school system or individual data attached to a Statewide Student Identifier.

"Personal Information" ("PI") is defined in Ohio Educ. Code §§ 1349-19 as "an individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: SSN; driver's license number or state identification card number; account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account."

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes. But the State does not possess individual student data in the first instance.

The statewide Education Management Information System (EMIS) is the Department of Education's ("DOE") student data system. Data submitted to the statewide Education Management Information System (EMIS), include individual test, attendance, demographic, program and course data. Such data are reported using a Statewide Student Identifier.

Ohio Revised Code § 3301.0714.

The reporting of a student's PI (name, address, social security number) is generally prohibited.

Ohio Revised Code § 3301.0714 (D)(1).

If so, are there exceptions?

The Ohio DOE empowers the Superintendent of Public Instruction to conduct studies and research projects for the improvement of public education, and to contract with third parties to conduct those studies. Such studies can include analysis of student data contained in the EMIS. Such student data may only identify students by the Statewide Student Identifier number, and no third party shall have access to the student's PI (name, address, SSN).

Ohio Revised Code § 3301.12(A)(3)

There may be limited instances where a name is reported to the DOE such as: (1) to allow the Ohio DOE to respond to a test score appeal or follow up when a student's written response to a test question includes threats or describes harm to the student or others; (2) where individual student data records collected and maintained for early childhood programs; (3) administration of various scholarship programs; and (4) calculation of a payment to a county board of developmental disabilities.

Ohio Revised Code § 3317.20

Data Minimization

Are there data retention limits?

The Ohio Office of Information Technology, IT Policy-E.30 governing electronic records sets forth guidelines requiring State agencies to employ records management procedures that govern the maintenance, preservation and destruction of data, among other things.

Where student data is shared with other state agencies, vendors, researchers and service providers, a formal memorandum of understanding is used to govern the use of the data. The memorandum requires that the data shared under the agreement be destroyed when the research study is complete.

Retention periods shall be established to ensure the deletion of PI which is no longer necessary for or relevant to the performance of lawful functions.

Ohio Administrative Code § 3301-2-05 (C)

Ohio (continued)

In the special education context, the public agency must inform parents when personally identifiable information ("PII") that has been collected, maintained, or used under this rule is no longer needed to provide educational services to the child. When notified… parents may request that the PII be destroyed, and the agency must comply. However, the agency must maintain a permanent record of the child's name, address, telephone number, grades, attendance record, classes attended, grade level completed and year completed (if applicable). Records that include PII about a child should be maintained for several years after graduation. If a child moves before graduation, the agency should keep those records until the child may have graduated. A year before a district plans to destroy records, the district should notify the parents and the child that the child's records are about to be destroyed, except for those kept as a permanent record, so that parents or children can request that certain records be kept.

Ohio Administrative Code § 3301-51-04.

Security

Is there a mandated data security program or specific security protocols?

Yes. The Ohio Privacy and Security Office provides guidance to all state agencies on protecting the privacy of Ohio's data and security. Under State of Ohio Administrative Policy IT-14 the requirements for securing sensitive data and information are:

- Identify and Label Sensitive Data: Agencies must classify data, systems, media, devices and electronic transmissions that comply with Ohio's data classification policy.
- Use of State Approved Strong Encryption: Agencies must use encryption that conforms to Ohio state encryption standards, which incorporate, in part, National Institute of Standards and Technology ("NIST") requirements.
- Secure Sensitive Data in Transmission: Agencies must encrypt data in transit and provide a process to check data in transit that risk unauthorized access to or disclosure of sensitive data.
- Secure Sensitive Data at Rest: At a minimum, agencies must encrypt data at rest. Agencies must also restrict the downloading of sensitive data, implement authorization controls, validate user account and deactivate former employee accounts.
- Secure Backups: For data backups and restorations, agencies must encrypt, implement access controls, reuse or destroy backup media in according with NIST guidelines and implement appropriate physical security controls such as limiting access, and providing secure transport and storage.
- Secure Sensitive Data on Portable Devices and Media: For sensitive data on portable devices and media, agencies must implement controls for the placement of sensitive data on portable devices and media, such as conducting risk assessments for a given device or type of media, requiring written authorization for placing sensitive data on portable device and media, written acknowledgement that the security requirements are being complied with, use of encryption and strong passwords to protect the sensitive data on the device and media, implement a procedure for the removal and destruction of sensitive data that conforms with NIST guidelines and Ohio state policies (ITP-E.1), and prohibiting the placement of sensitive data on portable, non-state owned devices.
- Physically Secure Sensitive Data: Agencies must ensure that only authorized personnel are allowed to access or remove devices containing sensitive data.
- Communicate Expectations for Handling Sensitive Data: Agencies must ensure that public servants are aware of and agree in writing to take precautions to protect sensitive data.

Note that Agencies may be allowed an exception from these security protocols if formally requested through the Department of Administrative Services Office of Information Security & Privacy. Any request must provide the technical and business justification for the exception and identify the potential risks and steps to mitigate those risks.

In addition, the Ohio Privacy and Security Office provides the Ohio DOE with a full-time chief information security officer to ensure compliance with Ohio law and policies.

Ohio Data Privacy Report

Is there required de-identification or aggregation of data?

Yes. PI appears to be collected by the individual school districts and community schools upon enrollment and submitted to a third party vendor to assign the unique data verification number (Statewide Student Identifier).

Ohio Revised Code § 3301.0714 (D)(2)

The state board shall annually compile the data reported by each school district. The state board shall design formats for profiling each school district as a whole and each school building within each district and shall compile the data in accordance with these formats. These profile formats shall: 1) Include all of the data gathered under this section in a manner that facilitates comparison among school districts and among school buildings within

Ohio
(continued)

each school district, 2) Present the data on academic achievement levels as assessed by the testing of student achievement.

Ohio Revised Code § 3301.0714

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Yes. Ohio Revised Code § 1347.15 requires that the director of a State agency designate an employee of the agency to serve as the data privacy point of contact within the agency to work with the chief privacy officer within the office of information technology to ensure that confidential PI is properly protected and that the agency complies with the rules protecting the confidentiality of PI.

Ohio Revised Code § 1347.15(A)(7)

In addition, the DOE has recommended that Ohio Revised Code § 3301.133 be revised to require a formal, identified unit to manage education data.

Ohio Data Privacy Report.

Further, Ohio Revised Code § 3301.0713 does mandate that the EMIS advisory board be established. The board is responsible for making recommendations to the DOE for improving the operation of the educational management information system. Topics that may be addressed by the recommendations include the definitions used for the data maintained in the system, reporting deadlines, rules and guidelines for the operation of the system adopted by the state board of education, and any other issues raised by education personnel who work with the system.

Is there a complaint process for student/parents when the law has been violated?

Not specified by statute.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified by statute.

Oklahoma

Applicable Laws

Title 70 of Okla. Stat. governs Schools

Key Provisions: Okla. Stat. tit. 70, § 3-168 (Student Data Accessibility, Transparency, and Accountability Act of 2013)

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education(al) records" means those official records, files, and data directly related to a student and maintained by the school or local education agency including, but not limited to, records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

Okla. Stat. tit. 70, § 510.1

"Covered Information" or "Student Data"

"Student data" means data collected and/or reported at the individual student level included in a student's educational record.

"Student data" includes: state and national assessment results, including information on untested public school students; course taking and completion, credits earned, and other transcript information; course grades and GPA; DOB, grade level and expected graduation date/cohort; degree, diploma, credential attainment, and other school exit information such as General Educational Development and drop-out data; attendance and mobility; data required to calculate the federal 4-year adjusted cohort graduation rate, including sufficient exit and drop-out information; discipline reports limited to objective information sufficient to produce the federal Title IV Annual Incident Report; remediation; special education data; demographic data and program participation information; and military student identifier.

Unless included in a student's educational record, "student data" shall not include: juvenile delinquency records; criminal records; medical and health records; student SSN; and student biometric information

Okla. Stat. tit. 70, § 3-168

"Directory information" includes a student's name, address, telephone listing, 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, degrees and awards received, and the most recent previous educational institution attended by the student.

Okla. Stat. tit. 51, § 24A.16

Use Limitations

Is sharing student data with third parties limited or prohibited?

The Oklahoma Board of Education ("BOE") is tasked with developing and publishing policies and procedures to comply with the Family Educational Rights and Privacy Act ("FERPA") and other relevant privacy laws and policies, and is specifically tasked with creating policies and procedures limiting how student data may be accessed and distributed in either an aggregated/de-identified form or not.

Okla. Stat. tit. 70, § 3-168

No institution within the Oklahoma State System of Higher Education or technology center school within the state system of career and technology education shall enter into any agreement to sell student data to any creditor for purposes of marketing consumer credit to students.

Okla Stat. tit. 70, § 3245

If so, are there exceptions to these limitations?

Specific codified exceptions to these limitations are not apparent.

Data Minimization

Are there data retention limits?

The BOE is tasked with developing a detailed data security plan that includes data retention and disposition policies.

Okla. Stat. tit. 70, § 3-168

The original copy of individual scholastic and other permanent student records shall be filed and permanently retained by the respective public schools of Oklahoma.

Olka. Stat. tit. 70, § 24-114

Security

Is there a mandated data security program or specific security protocols?

The BOE is tasked with developing a detailed data security plan that includes:

- guidelines for authorizing access to the student data system and to individual student data including guidelines for authentication of authorized access,
- privacy compliance standards,
- privacy and security audits, breach planning, notification and procedures, and
- data retention and disposition policies.

Okla. Stat. tit. 70, § 3-168

The BOE shall ensure that any contracts that govern databases, assessments or instructional supports that include student or de-identified data and are outsourced to private vendors include express provisions that safeguard privacy and security and

Oklahoma
(continued)

include penalties for noncompliance.

Okla. Stat. tit. 70, § 3-168

Is there required de-identification or aggregation of data?

Okla. Stat. tit. 70 § 3-168 dictates situations in which student data can or must be disclosed in an aggregated or de-identified form.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

A CPO requirement is not apparent.

Is there a complaint process for student/parents when the law has been violated?

A codified a complaint process for violations of student privacy is not apparent.

Is there a private right of action?

Not Applicable

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Any educational agency or institution making public directory information shall give public notice of the categories of information which it has designated as directory information with respect to each student attending the institution or agency and shall allow a reasonable period of time after the notice has been given for a parent to inform the institution or agency that any or all of the information designated should not be released without prior consent of the parent or guardian or the student if the student is eighteen (18) years of age or older.

Okla. Stat. tit. 51, § 24A.16

Oregon

Applicable Laws

Title 20 of Or. Rev. Stat. governs Education and Culture

Key Provisions: Or. Rev. Stat. § 326.565, et seq. governs Student Records (note: Oregon has passed legislation amending these provisions, effective July 2021, which is not included here);

Oregon SB 187 (Oregon Student Information Protection Act, effective July 1, 2016, to be codified at Or. Rev. Stat. § 646.607 – 646.652)

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education records" means official records, files, and data directly related to a student and maintained by the school or local education agency, including but not limited to records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Or. Rev. Stat. §110.1

"The education records shall include any education records relating to the particular student retained by an education service district."

Or. Rev. Stat. § 365.575

The State Board of Education ("BOE") may adopt by rule standards for the content and format of an Oregon electronic student record.

Or. Rev. Stat. § 326.580

"Covered Information" or "Student Data"

"Covered information" means personally identifiable information or materials that regard a student in this state and that are in any media or format that meet any of the following:

- Are created or provided by a student, or the student's parent or legal guardian, to an operator in the course of the student's, parent's or legal guardian's use of the operator's site, service or application for kindergarten through grade 12 purposes;
- Are created for an operator or provided to an operator by an employee or agent of the kindergarten through grade 12 school, school district or education service district for kindergarten through grade 12 purposes; or
- Are gathered by an operator and personally identify a student, or are linked to information that personally identifies a student, including, but not limited to: Information in the student's educational record or electronic mail; The student's first and last name, home address, telephone number, electronic mail address or other information that allows physical or online contact; or the student's discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, Social Security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photographs, voice recordings or geolocation information.

Oregon SB 187, § 2(2)(a)

Use Limitations

Is sharing student data with third parties limited or prohibited?

A public university may not disclose the Social Security number of a student who is attending the public university.

Or. Rev. Stat. § 326.587.

The same is true for community colleges.

Or. Rev. Stat. § 326.589

A public school or school district shall disclose personally identifiable information or other information allowed to be disclosed by the Family Educational Rights and Privacy from an education record of a student to: (a) law enforcement, child protective services, and health care professionals in connection with a health or safety; and (b) courts and state and local juvenile justice agencies including, but not limited to, law enforcement agencies, juvenile departments and child protective service agencies.

Or. Rev. Stat. § 336.187

An operator of a website, online service, or application directed at K-12 school purposes ("an operator") may not engage in targeted advertising in the website, online service, or application, target advertising on any other site, service, or application where the targeting is based on information acquired through the use of the operator's [services], sell a student's information or otherwise disclose a student's information (subject to caveats).

Oregon SB 187, § 2(3)(a)

If so, are there exceptions?

A public university may disclose a student's Social Security number at the request of law enforcement, after obtaining written consent from the student, in the payment or wages or benefits, in the payment or collection of taxes or a debt, or for purposes of statistical analysis.

Or. Rev. Stat. § 326.587. (The same is true for community colleges, codified at Or. Rev. Stat. § 326.589)

Under, Oregon SB 187, §§ 2(3)(a)(E),

Oregon (continued)

2(3)(b), and 2(5 – 7), an operator may disclose covered information in certain circumstances.

Data Minimization

Are there data retention limits?

The State BOE shall adopt by rule standards for the creation, use, custody and disclosure, including access, of student education records that are consistent with the requirements of applicable state and federal law.

Or. Rev. Stat. § 326.565

An operator shall delete a student's covered information within a reasonable time if the school or school district requests deletion of data that is under the control of the school district.

Oregon SB 187, § 4(b

Security

Is there a mandated data security program or specific security protocols?

An operator shall implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information and appropriate to protect the covered information from unauthorized access, destruction, use, modification or disclosure.

Oregon SB 187, § 4(a)

Is there required de-identification or aggregation of data?

Under Oregon SB 187, § 6(a & b), aggregated and de-identified student data may be used and disclosed by an operator in certain circumstances, including to demonstrate the effectiveness of the operator's offerings and to support the development and improvement of educational sites, services, or applications.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Oregon does not appear to have codified such a requirement.

Is there a complaint process for student/parents when the law has been violated?

Each educational institution that has custody of the student's education records shall annually notify parents and eligible students of their right to review and propose amendments to the records. The State BOE shall specify by rule the procedure for reviewing and proposing amendments to a student's education records. If a parent's or eligible student's proposed amendments to a student's education records are rejected by the educational institution, the parent or eligible student shall receive a hearing on the matter. The State BOE Education shall specify by rule the procedure for the hearing.

Or. Rev. Stat. § 326.575

Is there a private right of action?

A student who suffers an ascertainable loss of money, personal property, or real property as a result of a violation of Or. Rev. Stat. §§ 326.587 or 326.589 (both governing impermissible disclosure of Social Security number) may bring an action in a circuit court to recover the student's actual damages. The court may award reasonable attorney fees to the party that prevails in an action on a claim under this section.

Or. Rev. Stat. § 326.591

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

An educational institution may not use information authorizing access to a student's social media account that was obtained through the application of the educational institution's policies governing the use of university equipment or computer networks owned or operated by the educational institution without the voluntary consent of the student.

Or. Rev. Stat. § 326.551

Pennsylvania

Applicable Laws

Pennsylvania Data Access and Use Policy (as enabled under 22 Pa. Code §12.31 and 12.32)

Definitions

"Educational Records"

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education(al) records" means: those official records, files, and data directly related to a student and maintained by the school or local education agency, including, but not limited to, records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

22 Pa. Code ARTICLE II

"Covered Information" or "Student Data"

The Pennsylvania Data Access and Use Policy defines "personally identifiable student level data and/or information includes" as a "student's name; the name of the student's parent/guardian; the address of the student or student's family; personal identifiers; personal characteristics or other information that would make the student's identity easily traceable."

In the context of Private Licensed Schools, "Student records must contain a transcript of academic performance, which includes student name, identifying number, program or course attended, grades for all subjects taken, date of entrance, date of graduation or withdrawal and the award received upon completion."

22 Pa. Code § 73.21

Schools teaching any grades K through 12 shall maintain a permanent cumulative record for each student, which shall include the following:

- The number of hours of instruction received in each subdivision of the curriculum.
- Attendance.
- Scholastic achievement.
- Test scores.
- Data on personal characteristics, student health and co-curricular activities.

22 Pa. Code § 51.72

Use Limitations

Is sharing student data with third parties limited or prohibited?

Under the Data Access and Use Policy the Pennsylvania Department of Education ("PDE") may not disclose personally identifiable information to a third party researcher except in certain limited situation (described below).

If so, are there exceptions?

PDE may disclose PII to third party researchers if:

- The researcher is acting as an authorized representative of the PDE acting under the direct control of the PDE as an employee, appointed official or contractor who is providing services that the PDE would otherwise provide for itself;
- If the researcher is conducting authorized studies for or on behalf of the PDE to develop, validate or administer predictive tests; administer student aid programs or improve instruction.

In addition, any release of PII is subject to the following conditions:

- The party to whom the data are released does not disclose the information to any third party without prior written consent of parent or eligible student;
- The data will be used for the purpose for which the disclosure was made; and
- The data are destroyed when no longer needed for the purposes under which the disclosure was granted.

Data Minimization

Are there data retention limits?

Pennsylvania does not appear to have codified such limits with respect to K-12 educational records.

Security

Is there a mandated data security program or specific security protocols?

According to the Data Access and Use Policy, Pennsylvania has implemented technical measures to ensure the security of student records including:

- secure firewalls;
- secure socket layers;
- audit trails; and
- physical security, such as restricted server room access.

Is there required de-identification or aggregation of data?

Under the Data Access and Use Policy, the PDE uses student data to produce aggregate reports from individual data that relate to groups of students, rather than individual students. Student data will also be linked to other PDE databases to produced additional aggregate reports.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

There is no specific requirement. However, the Pennsylvania Data Access and Use Policy indicates that the Secretary of Education functions as the custodian of the data with the PDE.

Pennsylvania
(continued)

Is there a complaint process for student/parents when the law has been violated?

Not specified by statute.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified by statute.

Rhode Island

Applicable Laws

Title 16 of R.I. Gen. Laws governs Education

Key Provisions: R.I. Gen. Laws § 16-71-1, et seq. (the Rhode Island Educational Records Bill of Rights)

Definitions

"Educational Records"

The Rhode Island Educational Records Bill of Rights defines "records" in accordance with the definition of "education records" contained in the Family Educational Rights and Privacy Act ("FERPA").

R.I. Gen. Laws § 16-71-6

Pursuant to the Interstate Compact on Educational Opportunity for Military Children, "Education or educational records" means those official records, files, and data directly related to a student and maintained by the school or local education agency, including, but not limited to, records encompassing all the material kept in the student's cumulative folder such as general identifying data, records of attendance and of academic work completed, records of achievement and results of evaluative tests, health data, disciplinary status, test protocols, and individualized education programs.

R.I. Gen. Laws § 16-92-3

"Covered Information" or "Student Data"

In the context of student data-cloud computing, "student data" means any information in any media or format created or provided: (i) By a student; or (ii) By a school board employee about a student in the course of using a cloud computing service, including the student's name, email address, postal address, email message, documents, unique identifiers, and metadata.

R.I. Gen. Laws § 16-104-1

Use Limitations

Is sharing student data with third parties limited or prohibited?

Any person "who provides a cloud computing service to an educational institution" can "process data of a K-12 student for the sole purpose of providing cloud computing service" to the given institution and "shall not process such data for any commercial purposes," including, but not limited to, advertising purposes that benefit said provider. Every cloud computing service that enters into a contract to provide services to an educational institution must "certify, in writing, that it will not violate this provision."

R.I. Gen. Laws § 16-104-1

Parents, legal guardians, and students over 8 have the right to have educational records kept confidential and not released to any other individual, agency, or organization without prior written consent, except to the extent that such disclosures are authorized by FERPA "or other applicable law or court process."

R.I. Gen. Laws 16-71-3

If so, are there exceptions?

Rhode Island does not appear to have codified specific exceptions beyond the above.

Data Minimization

Are there data retention limits?

Every agency controlling public records must "prepare and submit records control schedules to the public records administration program, with the advice of the offices of the attorney general and auditor general."

R.I. Gen. Laws § 38-3-6

Security

Is there a mandated data security program or specific security protocols?

With the executive branch a "children's cabinet" is to be established, and one aspect of their work will be to "develop a strategic plan to coordinate and share data to foster interagency communication, increase efficiency of service delivery, and simultaneously protect children's legitimate expectations of privacy and rights to confidentiality. This shall include data-sharing with research partners, pursuant to data-sharing agreements, that maintains data integrity and protects the security and confidentiality of these records. Any such data-sharing agreements shall comply with all privacy and security requirements of federal and state law and regulation governing the use of such data." Further, any universal student identifier now in use by the state or developed in the future will not involve a student's social security number.

R.I. Gen. Laws § 42-72.5-2

Is there required de-identification or aggregation of data?

Not specified by statute.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Not specified by statute.

Is there a complaint process for student/parents when the law has been violated?

Any person aggrieved under the Rhode Island Educational Records Bill of Rights shall have the right to appeal in accordance with the provisions of chapter 39 of title 16. R.I. Gen. Laws § 16-71-3

R.I. Gen. Laws. §§ 16-39-1, et seq. outline a complaint process for any person aggrieved by any decision or doings of any school committee or in any other matter arising under any law relating to schools or education,

Rhode Island
(continued)

including through legal review.

Is there a private right of action?

See above.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

The parent, legal guardian, or eligible student shall have the right to have educational records kept confidential and not released to any other individual, agency, or organization without prior written consent of the parent, legal guardian or eligible student, except to the extent that the release of the records is authorized by the provisions of FERPA or other applicable law or court process.

R.I. Gen. Laws § 16-71-3

South Carolina

Applicable Laws

South Carolina Code 1976 § 59-1-490 ("South Carolina Department of Education Data Use and Governance Policy")

Applies only to South Carolina Department of Education

Definitions

No Defined Terms

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes. The South Carolina Department of Education may not share any personally identifiable individual student data in federally required reporting.

If so, are there exceptions?

Not specified by statute.

Collection Limitations

Does the state limit or prohibit the collection of student data?

Yes. The South Carolina Department of Education may not collect individual student data directly from students or families, except as required to meet its obligations under the Individuals with Disabilities Education Act. Each student is assigned a unique student identifier upon enrollment into the student management system to ensure compliance with the privacy rights of the student and his parents or guardians.

Data Minimization

Are there data retention limits?

Not specified by statute.

Security

Is there a mandated data security program or specific security protocols?

Yes. Data collected by the South Carolina Department of Education must be maintained within a secure infrastructure environment. Access to this data must be limited to pre-identified staff who are granted clearance related to their job responsibilities of federal reporting, state financial management, program assessment, and policy development. Training in data security and student privacy laws must be provided to these specific individuals on a regular basis in order to maintain their data use clearance along with a signed Data Use Policy assurance of confidentiality and privacy.

Is there required de-identification or aggregation of data?

Yes, in certain circumstances. All data elements collected and transferred from the South Carolina State Department of Education to the United States Department of Education must be based on the reporting requirements contained in EDFacts (a U.S. Department of Education performance data initiative), or other federal laws and regulations, and only may include aggregated data with no personally identifiable data.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Not specified by statute.

Is there a complaint process for student/parents when the law has been violated?

Not specified by statute.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified by statute.

South Dakota

Applicable Laws

SDCL § 13-3-51 "Data reporting and record systems"

Applies only to the South Dakota Department of Education

Definitions

"Educational Records"

As defined in 34 C.F.R. § 99.3:

"**(a)** The term means those records that are:

(1) Directly related to a student; and

(2) Maintained by an educational agency or institution or by a party acting for the agency or institution."

"Personally Identifiable Information"

As defined in 34 C.F.R. § 99.3:

"The term includes, but is not limited to--

(a) The student's name;

(b) The name of the student's parent or other family members;

(c) The address of the student or student's family;

(d) A personal identifier, such as the student's social security number, student number, or biometric record;

(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

(f) Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

(g) Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates."

"Aggregate Data"

"Information from education records in which all personally identifiable information has been removed."

Use Limitations

Is sharing student data with third parties limited or prohibited?

The South Dakota Department of Education may not, as part of any reporting requirement tied to federal funds, report personally identifiable information from education records to the United States Department of Education.

If so, are there exceptions to these limitations?

The law makes an exception for information required to be reported pursuant to 20 U.S.C. § 6398 to improve programs for migrant students.

Data Minimization

Are there data retention limits?

No.

Security

Is there a mandated data security program or specific security protocols?

The South Dakota Department of Education must develop security measures and procedures intended to protect personally identifiable information from release to unauthorized persons or for unauthorized purposes. Any collection, maintenance, or disclosure of education records by the department must comply with privacy protection laws in all respects including the:

• Family Educational Rights and Privacy Act (20 U.S.C. 1232(g));

• Protection of Pupil Rights Amendment (20 U.S.C. 1232(h)); and the

• Individuals with Disabilities Education Act (20 U.S.C. 1401 et seq.)).

Is there required de-identification or aggregation of data?

No, but the disclosure of "aggregate data" (defined above) is not prohibited by this law.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Not specified by statute.

Is there a complaint process for student/parents when the law has been violated?

Not specified by statute.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

No, but no elementary school or secondary school student can be required to submit to a survey, analysis, or evaluation. Without the written consent of the student or their parent/guardian that reveals information concerning:

(1) Political affiliations or beliefs of the student or the student's parent;

(2) Mental or psychological problems or aspects of the student or the student's family;

(3) Sex behavior or attitudes of the student or the student's family;

(4) Illegal, anti-social, self-incriminating, or demeaning behavior;

(5) Critical appraisals of other individuals with whom respondents have close family relationships;

(6) Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;

(7) Religious practices, affiliations, or beliefs of the student or student's parent;

(8) Personal or family gun ownership; or

South Dakota

(9) Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program)

Tennessee

Applicable Laws

Tenn Code §§ 49-1-702; 49-1-703; 49-1-704; 49-1-705; 49-1-706; 10-7-504; 10-7-509

Definitions

"Educational Records"

Undefined.

"Covered Information" or "Student Data"

"Student data" is defined as data collected or reported at the individual student level that is included in a student's educational records, including: state and national assessment results, including information on untested public school students; course taking and completion, credits earned and other transcript information; course grades and GPA; DOB, grade level and expected graduation date/cohort; degree, diploma, credential attainment and other school exit information such as receipt of the GED (R) and drop-out data; attendance and mobility; data required to calculate the federal four year adjusted cohort graduation rate, including sufficient exit and drop out information; discipline reports limited to objective information sufficient to produce the federal Title IV annual incident report; remediation; special education data; and demographic data and program participation information: juvenile delinquency records, criminal records, medical and health records, student social security number, and student biometric information.

Tenn. Code § 49-1-702(9)

"Biometric data" is also defined as a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition or an individual.

Tenn. Code § 49-1-702(2)

Use Limitations

Is sharing student data with third parties limited or prohibited?

The State must treat the records of students in public educational institutions as confidential. Information in such records relating to academic performance, financial status of a student or the student's parent or guardian, medical or psychological treatment or testing shall not be made available to unauthorized personnel of the institution or to the public or any agency, except those agencies authorized by the educational institution to conduct specific research or otherwise authorized by the governing board of the institution, without the consent of the student involved or the parent or guardian of a minor student attending any institution of elementary or secondary education, except as otherwise provided by law or regulation pursuant thereto, and except in consequence of due legal process or in cases when the safety of persons or property is involved.

Statistical information not identified with a particular student may be released to any person, agency, or the public; and information relating only to an individual student's name, age, address, dates of attendance, grade levels completed, class placement and academic degrees awarded may likewise be disclosed.

Tenn. Code § 10-7-504(a)(4)(A).

The State must restrict access to student data and de-identified data in the student data system to the following third parties: Department of Education ("DOE") and LEA contractors and/or researchers, parents, entities in compliance with subpoena or court order, or in connection with an interagency audit or evaluation of an education program. The State is also prohibited from transferring student or de-identified confidential data to any out-of-state organization, entity or agency, except in certain limited circumstances.

Tenn. Code § 49-1- 703(2)(A)

Parents and guardians have the right to inspect, review, collect and request student data related to their children's educational records.

Tenn. Code § 49-1-704(a)-(c)

If so, are there exceptions?

The State may transfer student and de-identified confidential data to an out-of-state organization, entity, or agency, if a student transfers out-of-state, an LEA need assistance locating an out-of-state transfer, a student leaves the state to attend an out-of-state institution of higher education or training program, a student registers for or takes a national or multistate assessment, a student voluntarily participates in a program where a data transfer is a requirement, the DOE enters into a contract governing databases, assessment, special education or instructional supports with an out-of-state vendor or a student is classified as a migrant for federal reporting purposes.

Tenn. Code § 49-1-703

The State must ensure that any contracts that govern databases, assessments, or instructional supports that include student or de-identified data and are outsourced to private vendors include express provisions that safeguard privacy and security and include penalties for noncompliance.

Tenn. Code § 49-1-703

The governing board of the institution, the DOE, and the Tennessee higher education commission shall have access on a confidential basis to student records as are required to fulfill their lawful functions.

Tenn. Code § 10-7-504(a)(4)(A).

Tennessee
(continued)

Data Minimization

Are there data retention limits?

The disposition of all state records shall occur only through the process of an approved records disposition authorization. Records authorized for destruction shall be disposed of according to the records disposition authorization and shall not be given to any unauthorized person, transferred to another agency, political subdivision, or private or semiprivate institution.

Tenn. Code § 10-7-509

The disposition of all state records shall occur only through the process of an approved records disposition authorization. Records authorized for destruction shall be disposed of according to the records disposition authorization and shall not be given to any unauthorized person, transferred to another agency, political subdivision, or private or semiprivate institution.

Tenn. Code § 10-7-50

Security

Is there a mandated data security program or specific security protocols?

The State is required to develop a detailed data security plan that includes: guidelines for authorizing access to the teacher and student data and data system; privacy compliance standards; privacy and and security audits; breach planning; notification and procedures; and data retention and disposition policies.

Tenn. Code § 49-1- 703 (3)(B)

Is there required de-identification or aggregation of data?

The State only uses aggregate data in public reports or in response to public record requests relating to the State's data security plan.

Tenn. Code § 49-1- 703 (2)(B)

The State may only use aggregate data in the release of data in response to research and data requests, unless otherwise permitted or unless the State provides specific approval for the release of student or de-identified data.

Tenn. Code § 49-1-703 (2)(C)(b)(ii)

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Tennessee does not appear to have codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

Tennessee does not appear to have codified such a process.

Is there a private right of action?

Not specified by statute.

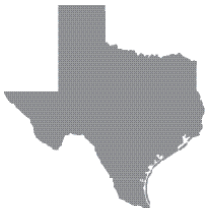
Individual Participation

Are parents/students able to opt-out of data collection or sharing?

There does not appear to be an opt-out for parents or students from data collection or sharing. However, parents and students must opt-in i.e. provide consent to the collection of biometric data.

Tenn. Code § 49-1-706

Texas



Applicable Laws

Tex. Educ. Code:

§1.005 Sharing Student Information

§7.008 Public Access to PEIMS data (really, TSDS).

§7.010 Electronic Student Records System

§42.006 Public Education Information Management System

Texas Admin. Code (TAC):

13 TAC §7.125(a)(6) Retention Schedule for Records of Public School Districts

1 TAC §202.1 Information Security Standards

Tex. Gov. Code:

§552.114 Student Records Exception to public information requests- Information in student records at an educational institution partially or wholly funded by state revenue is confidential. It can only be made available at the request of an education institution personnel, student or student's parent or legal guardian or spouse, or a person conducting a child abuse investigation under the law (Family Code).

Definitions

"Educational Records"

Taken from the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g (FERPA): Records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution.

"Covered Information" or "Student Data"

Unclear, §7.010(c) appears to include:

- Course or grade completion
- Teachers of record
- Assessment of instrument results
- Receipt of special education services
- Personal graduation plan

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes, via Tex. Gov. Code §552.114.

The Texas Student Data System also states that they do not share data with third party vendors (or sell data to third party vendors).

If so, are there exceptions?

Tex. Gov. Code §552.114 allows student data to be available only at the request of:

- education institution personnel;
- student or student's parent or legal guardian or spouse; or
- a person conducting a child abuse investigation under the law

The Texas Student Data System has exceptions for mandated sharing with other organizations and entities, and to the government for reporting purposes.

TEA shares anonymous aggregated data with the public.

Data Minimization

Are there data retention limits?

Yes. The Retention schedule (linked under Data Minimization) sets out mandatory retention periods and exceptions. See pages 8-12 of the Records Retention document.

Data for Missing Persons files (photographs and fingerprints) must be given back to the parents or guardians of the student. If they cannot be returned they must be destroyed.

Unsure as to the Texas Student Data System.

Security

Is there a mandated data security program or specific security protocols?

Yes. Requires particular programming provided in the Texas Educational Data Standards (TEDS).

Also IBM Tivoli Identity Mgmt. Platform.

Two state sponsored student information system vendors providing security for user access and hosting.

TEA is directly hosting TSDS at Texas Data Centers.

It appears that TSDS is in compliance with other provisions of TAC about information security services (Such as 202.1).

Is there required de-identification or aggregation of data?

Yes. TSDS uses FERPA and HIPAA de-identification and aggregation where necessary.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Appears to require a Data Steward for LEAs (local education agencies, which include the public school districts). Does not speak to any other companies receiving student data.

Is there a complaint process for student/parents when the law has been violated?

No clear avenue, but a likely path is to go through the Texas Education Agency's complaint pages or a local District Attorney.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified by statute.

Utah

Applicable Laws

Utah Code Ann. § 53A-1-413

Utah Code Ann. § 53A-13-301

Utah Code Ann. § 53A-1b-110

Utah Code Ann. § 53A-1-711

Definitions

"Student Achievement Backpack"

"Student Achievement Backpack" means, for a student from kindergarten through grade 12, a complete learner profile that: (i) is in electronic format; (ii) follows the student from grade to grade and school to school; and (iii) is accessible by the student's parent or guardian or an authorized LEA user. The Student Achievement Backpack shall include: (a) student demographics; (b) course grades; (c) course history; (d) results for an assessment administered under U-PASS; (e) section attendance; (f) the name of a student's teacher for classes or courses the student takes; (g) teacher qualifications for a student's teacher, including years of experience, degree, license, and endorsement; (h) results of formative, interim, and summative computer adaptive assessments; (i) detailed data demonstrating a student's mastery of the core standards for Utah public schools and objectives as measured by computer adaptive assessments; (j) a student's writing sample written for an online writing assessment; (k) student growth scores for U-PASS tests; (l) a school's grade assigned pursuant to Part 11, School Grading Act; (m) (n) results of benchmark assessments of reading administered; and (o) a student's reading level at the end of grade 3.

Utah Code Ann. § 53A-1-413

"LEA"

A school district, charter school, or the Utah Schools for the Deaf and the Blind.

Utah Code Ann. § 53A-1-413

"Authorized LEA user"

A teacher or other person who is: (i) employed by an LEA that provides instruction to a student; and (ii) authorized to access data in a Student Achievement Backpack through the Utah Student Record Store.

Utah Code Ann. § 53A-1-413

Use Limitations

Is sharing student data with third parties limited or prohibited?

Generally, not specified. But possibly in the near future because the code requires the chief privacy office to present recommendations on or before January 31, 2016.

Utah Code Ann. § 53A-1-711

In addition, where the board enters into a results-based contract with a private entity to fund education, the contract must include that the private entity is not eligible to receive or view any personally identifiable student data of students funded through a results-based contract. Further, the board shall ensure that the parent or guardian of an eligible student participating in a program funded pursuant to a results-based contract has given permission and signed an acknowledgment that the student's data may be shared with an independent evaluator for research and evaluation purposes.

Utah Code Ann. § 53A-1b-110

The state also requires that the State Board of Education make rules to establish standards for public education employees, student aides, and volunteers in public schools regarding the confidentiality of student information and student records.

Utah Code Ann. § 53A-13-301

The state specifies who can access a Student's Achievement Backpack. The following people shall have access: (i) the student's parent or guardian; and (ii) each LEA that provides instruction to the student.

Utah Code Ann. § 53A-1413

If so, are there exceptions?

Not specified by statute.

Data Minimization

Are there data retention limits?

Not specified. But possibly in the near future because the code requires the chief privacy office to present recommendations on or before January 31, 2016.

Utah Code Ann. § 53A-1-711

Not specified. But possibly in the near future because the code requires the chief privacy office to present recommendations on or before January 31, 2016.

Utah Code Ann. § 53A-1-711

Security

Is there a mandated data security program or specific security protocols?

Yes. The state specifies that the State Board of Education shall implement security measures to ensure that: (a) student data stored or transmitted to or from the Utah Student Record Store is secure and confidential pursuant to the requirements of the Family Educational Rights and Privacy Act, 20 U.S.C. Sec. 1232g; and (b) an authorized LEA user may only access student data that is relevant to the user's LEA or school.

Utah Code Ann. § 53A-1-413

Is there required de-identification or aggregation of data?

Not specified. But possibly in the near future because the code requires the chief privacy office to present recommendations on or before January 31, 2016.

Utah
(continued)

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Yes. The board shall designate a chief privacy officer. The chief privacy officer shall: (i) oversee the administration of student privacy laws; and (ii) work with the board to develop the funding proposal and recommendations on how the board and the Legislature can update student privacy laws in statute and in board rule.

Utah Code Ann. § 53A-1-711

Is there a complaint process for student/parents when the law has been violated?

Not specified. But possibly in the near future because the code requires the chief privacy office to present recommendations on or before January 31, 2016.

Utah Code Ann. § 53A-1-711

Is there a private right of action?

Not specified, but the code required the chief privacy office to present recommendations on or before January 31, 2016.

Utah Code Ann. § 53A-1-711

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified, but the code requires the chief privacy office to present recommendations on or before January 31, 2016.

Utah Code Ann. § 53A-1-711

Vermont

Applicable Laws

Vermont Department of Education Protection of Confidential Information Policy ("DOE" Policy") available

at: http://education.vermont.gov/documents/EDU-Data_Request_Confidentiality_Policies.pdf

Definitions

"Covered Information" or "Student Data"

Vermont does not appear to have any statue regulating student information. However, on September 19, 2008, the Department of Education approved a data suppression policy for student information that applies to all Vermont Department of Education contracts and reports as well as those generated by third parties working on its behalf. The DOE Policy includes the following definitions:

"Personally identifiable information" is information that alone, or in combination with other information, is linked, or is linkable, to a specific student, and which would thereby allow a reasonable person in the school or its community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

"Sensitive information" is any information which is protected under federal and/or state statute.

"Confidential information" is any information which is both "sensitive information" and "personally identifiable information."

Use Limitations

Is sharing student data with third parties limited or prohibited?

Not specified by statute, but the DOE Policy requires the state Department of Education to suppress aggregate student counts under certain circumstances.

All analysis of student-level data must take place on a Vermont Department of Education network, and personally identifiable student information may not be removed from a Vermont Department of Education network.

In addition, the Vermont Department of Education may enter into contracts or issue grants which result in contractor or grantee possession of confidential student information in electronic format so long as the contracts or grants are approved by the Commissioner and include the following:

- a description of the appropriate and allowable uses of the information;
- the scope of the information which will be permitted to be in the possession of the contractor or grantee;
- requirements for signed confidentiality agreements for all individuals having access to the system;
- minimum information technology security requirements as deemed appropriate by the Vermont Department of Education's Information Technology Director; and
- a description of the required process.

Other conditions which may be deemed necessary for the protection of confidential information may be required by the Commissioner or the Commissioner's designee.

If so, are there exceptions?

N/A

Data Minimization

Are there data retention limits?

Not specified by statute.

Security

Is there a mandated data security program or specific security protocols?

Not specified by statute.

See "Use Limitations" above for DOE Policy.

Is there required de-identification or aggregation of data?

Not specified by statute.

The DOE Policy requires that research which includes the analysis of personally identifiable student-level information which is also classified as sensitive must first be de-identified by Vermont Department of Education staff.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Not specified by statute.

Is there a complaint process for student/parents when the law has been violated?

Not specified by statute.

Is there a private right of action?

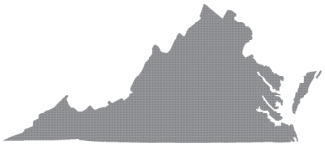
Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified by statute.

Virginia



Applicable Laws

VA ST § 22.1-20.2: Student Data Security

VA ST § 22.1-79.3 Policies Regarding Certain Activities

VA ST § 22.1-287.02 Students' personally identifiable information.

VA ST § 22.1-289 Transfer and management of scholastic records; disclosure of information in court notices; penalty

VA ST § 22.1-289.1 School service providers; student personal information

VA ST § 22.1-287 Limitations on access to records.

VA ST § 22.1-287.01 Student information; release to federal government agencies.

VA ST § 22.1-288 Furnishing information to public or private school, college or university, or private business or professional school or college or military force.

VA ST § 22.1-288.2 Receipt, dissemination and maintenance of certain law-enforcement information.

8 VAC 20-81-20 Definitions

8 VAC 20-81-170 Procedural Safeguards

Definitions

"Educational Records"

Educational Records: Defined using the Interstate Compact on Educational Opportunity for Military Children

§ 22.1- 360

Education Record: Means those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for the agency or the institution. The term also has the same meaning as "scholastic record". In addition to written records, this also includes electronic exchanges between school personnel and parent(s) regarding matters associated with the child's educational program. The term also includes records covered under the definition of "education record" in the regulations implementing the Family Educational Rights and Privacy Act ("FERPA") (e.g. 22.1-289).

8 VAC 20-81-10

Personally Identifiable Information: Uses the same definition as FERPA for personally identifiable information.

§ 22.1-287.01

Scholastic Record: records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. These include but are not limited to documentation pertinent to the educational growth and development of students as they progress through school, student disciplinary records, achievement and test data, cumulative health records, reports of assessments for eligibility for special education services, and individualized Education Programs.

Such records may be recorded in any way, including but not limited to, handwriting, print, computer media,

video or audio tape, film, microfilm, and microfiche.

§ 22.1-289

"Covered Information" or "Student Data"

Student personal information- information collected through a school service that identifies an individual student or is linked to information that identifies an individual student.

§ 22.1- 289.01

"Directory information" (per FERPA)- student's name, sex, address, telephone listing, 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, degrees and awards received and other similar information.

§ 22.1-287.1

Sexual information/ mental health information/ medical information/ information on student health risk behaviors/ controlled substance use/ sensitive in nature information as identified by school board for students requires notification in writing to parents thirty days prior to administration. The personnel administering surveys/ questionnaires regarding this material cannot disclose personally identifiable information.

§ 22.1-79.3

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes, under § 22.1-287.01 a member or employee of a local school board or the Department of Education ("DOE") cannot transmit personally identifiable information to a federal government agency or an authorized representative of such agency, except as required by federal law or regulation.

§ 22.1-287 also limits access to educational records.

If so, are there exceptions?

• De-identified information for research

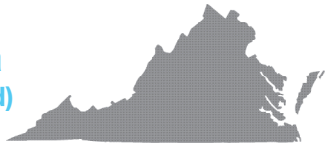
• Limited information to:

• An officer or employee of the U.S. government seeking information in the course of their duties when the pupil is a veteran, orphan or dependent of such veteran or an alien;

• An employee of local department of social services who needs the record to determine the eligibility of the pupil's family for public assistance and social services

• The juvenile justice system for service prior to adjudication- also to attorneys, court services units, juvenile detention centers or group homes,

Virginia (continued)



mental and medical health agencies, state and local children and family service agencies, and the Department of Juvenile Justice and the staff of such agencies.

But, prior to the disclosure for juvenile justice, the persons to whom the records are to be disclosed shall certify in writing to the principal or his designee that the information will not be disclosed to any other party, except as provided under state law, without prior written consent of the parent of the pupil or by such pupil if the pupil is 18 years of age or older.

§ 22.1-287

Directory information may be publicly released in accordance with federal law and the Board of Education regulations.

§ 22.1-287.1

Information may be furnished to public or private school, college or university, or private business or professional school or college or military force- name and addresses of pupils presently enrolled or pupils who have terminated their enrollment to any officer or employee of the entities above for the purposes of informing the pupils and former pupils of the educational and career opportunities available in the institutions or the military. No such entity can use the information for purposes not directly related to the academic or professional goals of the institution or the military force. Upon violation, the entities who receive the lists shall be suspended for two years from the discovery of list misuse.

§ 22.1-288

(A) A division superintendent shall disseminate the notice or information regarding an adjudication of delinquency or conviction…to school personnel responsible for the management of student records and to other relevant school personnel, including, but not limited to, the principal of the school in which the student is enrolled. The principal shall further disseminate such information to licensed instructional personnel and other school personnel who (i) provide direct educational or support services to the student and (ii) have a legitimate educational interest in such information.

(B) … [a] parent or guardian shall also be notified of his or her right to review, and to request an amendment of, the student's scholastic record, in accordance with regulations of the Board of Education governing the management of scholastic records; Superintendent shall provide information regarding the student's educational and attendance status to the intake officer or court services unit, as the case may be, upon receipt of the notice of filing of a petition from the intake officer in accordance with § 16.1- 260 or upon request of a court services unit for information made in conjunction with the preparation of a social history report pursuant to § 16.1.273.

§ 22.1-288.2

School service providers cannot use or share student personal information for behaviorally targeted advertisements to students, use or share student personal information to create a personal profile other than for supporting purposes. . . knowingly retain student personal information beyond the time authorized in the contract between the school and the service provider. . . sell student personal information.

§ 22.1-289.01

Data Minimization

Are there data retention limits?

Yes. Dictated by the retention schedules for the Library of Virginia.

Security

Is there a mandated data security program or specific security protocols?

Yes. The DOE, in collaboration with the Virginia Technologies Agency, shall develop and update regularly but in no case less than annually, a model data security plan for the protection of student data held by school divisions. Such model plan shall include (i) guidelines for access to student data and student data systems, including guidelines for authentication of authorized access; (ii) privacy compliance standards; (iii) privacy and security audits; (iv) procedures to follow in the event of a breach of student data; (v) data retention and disposition policies. The model plan and any updates shall be made available to every school division.

§ 22.1-20.2

Is there required de-identification or aggregation of data?

Names must be removed if the division superintendent provides information to universities, or development org or laboratory for research project or study.

§ 22.1-287(D)(1)

Auditing and Accountability

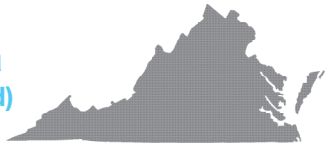
Is there a requirement for a CPO for either school districts or companies receiving student data?

Yes. The DOE shall designate a chief data security officer, with such state funds as made available to assist school divisions, upon request, with the development and implementation of their own data security plans and to develop best practice recommendations regarding the use, retention and protection of student data.

§ 22.1-20.02

Is there a complaint process for

Virginia
(continued)



student/parents when the law has been violated?

Not specified by statute.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified by statute.

Washington

Applicable Laws

28A.705.010 Compact Provisions.

28A.604.020 Student User Privacy in Education Act ("SUPER") Student Personal Information—Information about collection and use—Changes to privacy policies—Access to and correction of information—Application to education data center. Eff. July 1, 2016, SB5419: This law is for school service providers, which are providers that provide websites, mobile apps or online services for K-12 schools, used at the direction of teachers or employees at K-12 schools and collects, maintains or uses student personal information.

28A.300.500. Longitudinal student data system. (2) The confidentiality of personally identifiable student data shall be safeguarded consistent with the requirements of the federal family educational rights privacy act and applicable state law. Consistent with the provisions of these federal and state laws, data may be disclosed for educational purposes and studies, including but not limited to. . . (4) Nothing in this section precludes the office of the superintendent of public instruction from collecting and distributing aggregate data about students or student-level data without personally identifiable information.

28A.150.510. Transmittal of education records to department of social and health services-Disclosure of educational records- Data-sharing agreements- Comprehensive need requirement document-Report.

28A. 605.030.

28A.600.475

Definitions

"Educational Records"

In compact provisions (28A.705.010) Article II.E. "Education records" or "educational records" means those official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Also uses personal information (45.56.230) "Personal information in any files maintained for students in public schools, patients or clients of public institution or public health agencies, or welfare recipients" is exempt from public inspection and copying.

"Covered Information" or "Student Data"

"Student Personal Information"- information collected through a school service that personally identifies an individual student or other information collected and maintained about an individual student.

Use Limitations

Is sharing student data with third parties limited or prohibited?

SUPER: School service providers may not sell student personal information.

School service providers may not use or share any student personal information for purposes of targeted advertising to students.

"Education records may be shared with the department of social and health services upon request as long as the department certifies it won't disclose the education records to any other party without prior written consent of the student or parent unless authorized to disclose the records under state law." The department of social and health services is only authorized to disclose the education records it receives to a foster parent, guardian or other entity who is authorized to provide residential care to the student. "The department is also authorized to disclose educational records it obtains pursuant to this section to those entities with which it has contracted or with which it is formally collaborating, having responsibility for educational support services and educational outcomes of students who are dependent pursuant to chapter 13.34 RCW."

28A.150.510(1)

A school may not release the educational records of a student without the written consent of the student's parent or guardian, except as authorized by RCW 28A.600.475 and the Family Educational Rights and Privacy Act ("FERPA").

28A. 605.030.

School districts may participate in the exchange of information with law enforcement and juvenile court officials to the extent permitted by FERPA. When directed by court orders or pursuant to any lawfully issued subpoena, a school district shall make student records and information available to law enforcement officials, probation officers, court personnel and others legally entitled to the information. Except as provided in 13.40.480, parents and students shall be notified by the school district of all such orders or subpoenas in advance of compliance with them.

28A.600.475.

If so, are there exceptions?

SUPER: Sec. 4 (2). A third party can sell student personal information in a purchase, merger or other type of acquisition, or any assets of another entity, as long as the successor is subject to provisions of the section.

Sec. 4 (1). May collect, use or share information only for purposes

Washington (continued)

authorized by the relevant educational institution or teacher, or with the consent of the student or the student's parent or guardian.

Sec. 4 (6)(a)-(f). Exceptions for protecting integrity or security of its website, mobile site or online service; compliance; judicial process; protect the safety of other users or others on the web site, mobile application or online service; investigate a matter related to public safety; a subcontractor if the school service provider contractually prohibits the subcontractor from using the personal information for any purpose other than providing the contracted service to or on behalf of the school service provider (ii) prohibits the subcontractor from disclosing any student personal information provided by the school service provider to subsequent third parties unless the disclosure is expressly permitted….

Data Minimization

Are there data retention limits?

School service providers must delete student personal information within a reasonable period of time if the relevant educational institution requests deletion of the data under the control of the educational institution, unless: (a) the school service provider has obtained student consent or the consent of the student's parent or guardian to retain related to that student; or (b) the student has transferred to another educational institution and that educational institution has requested that the school service provider retain information related to that student.

28A.604.040. Sec. 5(2).

Also, data retention schedules.

SUPER: See Sec. 5(2) and the data retention schedules.

Security

Is there a mandated data security program or specific security protocols?

SUPER: Sec. 5 (1) School service providers must maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of student personal information. The information security should make appropriate use of administrative, technological, and physical safeguards.

Is there required de-identification or aggregation of data?

Yes, the data center de-identified data, but also is aggregated or disaggregated by ethnic groups for analysis (etc).

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Not specified by statute.

Is there a complaint process for student/parents when the law has been violated?

Not specified by statute.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified by statute.

West Virginia

Applicable Laws

§ 126-94-1 through § 126-94- 33 Procedures for the Collection, Maintenance and Disclosure of Student Data

§18-2-5h. Student Data Accessibility, Transparency and Accountability Act.

Definitions

"Educational Records"

"Education records" means those records that are directly related to a student and are collected, maintained or disclosed by an educational agency or institution or by a party acting for the agency or institution. This does not include teacher notes (not shared with others), law enforcement records, employment records, records by a health professional created in connection with provision of treatment to a student, and records of an educational agency or institution that contain only information related to a person after that person is no longer a student at the educational agency or institution, such as alumni records.

§ 126-94-4

"Covered Information" or "Student Data"

No definition.

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes. §§ 126-94-16 – 126-94-18; §§

126-94-20 – 126-94-25. An educational agency or institution shall obtain written consent of the parent of a student or the eligible student before disclosing personally identifiable information from the education records of a student, other than directory information.

If so, are there exceptions?

Yes. Under § 126-94-18, an educational agency or institution may disclose personally identifiable information from a student's education records without written consent if the disclosure is to:

- Other school officials;
- Certain authorized federal and state educational authorities (in connection with financial aid or for limited state and local reporting);
- Accrediting organizations;
- The parents of a dependent student;
- Comply with court order;
- For appropriate health and safety emergencies; and
- A social worker.

Data Minimization

Are there data retention limits?

No. An educational institution is not precluded from destroying records and may do so under certain circumstances, as outlined in 126-94-12. There are no guidelines as to limits. There are no requirements to delete information, but the district may do so after certain time limits, depending on the information.

§ 126-94-12.

Security

Is there a mandated data security program or specific security protocols?

A school district has the responsibility to immediately respond to any data privacy or security incidents or breaches and report such incidents to the appropriate authorities, including the WVDE Office of Legal Services and Accountability, for further response and investigation.

§ 126-94-3.4.a.5

Each participating agency shall protect the confidentiality of personally identifiable information at collection, storage, disclosure and destruction stages.

§ 126-94-27.1

Is there required de-identification or aggregation of data?

Any and all public reports and/or releases of student data when necessary to fulfill the requirements of state and/or federal laws, rules, and regulations will be presented in aggregate.

§ 126-94-16.1.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

West Virginia does not appear to have codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

A parent, eligible student, or school official may file a complaint with the WVDE Office of Legal Services and Accountability regarding an alleged violation under applicable privacy regulations.

§ 126-94-29

Is there a private right of action?

Yes.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

West Virginia does not appear to have codified an ability to opt-out of data collection or sharing.

Wisconsin

Applicable Laws

Wis. Stat. Ann. § 118.125 Pupil Records

Wis. Stat. Ann. § 115.297. Cooperative research on education programs; statewide student data system

Definitions

"Educational Records"

"Pupil records" means all records relating to individual pupils maintained by a school but does not include any of the following:

1. Notes or records maintained for personal use by a teacher or other person who is required to hold a certificate, license, or permit if such records and notes are not available to others.

2. Records necessary for, and available only to persons involved in, the psychological treatment of a pupil.

3. Law enforcement unit records.

§ 118.125

"Covered Information" or "Student Data"

"Student data" means information contained in education records, as defined in FERPA, and pupil records.

§ 115.297

Use Limitations

Is sharing student data with third parties limited or prohibited?

Yes. All pupil records maintained by a public school shall be confidential, with limited exceptions.

§ 118.125(2).

If so, are there exceptions?

Limited exceptions are made for law enforcement, authorized public officials, and to the parents of a pupil, or for limited purposes during an emergency.

§ 118.125(2).

Data Minimization

Are there data retention limits?

Yes. Each school board shall adopt rules in writing specifying the content of pupil records and the time during which pupil records shall be maintained. A pupil's progress records shall be maintained for at least 5 years after the pupil ceases to be enrolled in the school.

§ 118.125(3)

No behavioral records may be maintained for more than one year after the pupil ceases to be enrolled in the school, unless the pupil specifies in writing that his or her behavioral records may be maintained for a longer period.

§ 118.125(3)

Security

Is there a mandated data security program or specific security protocols?

Not specified by statute.

Is there required de-identification or aggregation of data?

Not specified by statute.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Not specified by statute.

Is there a complaint process for student/parents when the law has been violated?

Not specified by statute.

Is there a private right of action?

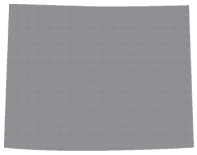
Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Not specified by statute.

Wyoming



Applicable Laws

Wyo. Stat. Ann. § 21-2-202

Definitions

"Educational Records"

No explicit definition.

"Covered Information" or "Student Data"

No explicit definition.

Use Limitations

Is sharing student data with third parties limited or prohibited?

There is no specific statute prohibiting the sharing of student data with third parties. However, the state requires that the State Superintendent establish a state security plan that prohibits the sale of student data to private entities or organizations. The relevant excerpts are below.

The State Superintendent, "for purposes of the statewide assessment of students and reporting student performance," has authority "to assess and collect student educational assessment data from school districts, community colleges and the University of Wyoming." The data "shall be consolidated, combined and analyzed in accordance with state law..."

Wyo. Stat. Ann. § 21-2-202

Under § 21-2-202, the State Superintendent, with the Department of Enterprise Technology Services has to "establish criteria for the collection, storage, management and reporting of department of education data related to teacher certification, statewide education accountability and assessment and the administration of the school finance system."

They must also develop a data security plan that includes:

- Guidelines for authorizing access to student data, including authentication of authorized access;
- Privacy compliance standards;
- Privacy and security audits;
- Breach planning, notification and procedures pertaining thereto;
- Data retention and disposition policies;
- Data security policies including electronic, physical and administrative safeguards such as data encryption and employee training;
- Routine and ongoing compliance with the federal Family Educational Rights and Privacy Act and other privacy laws and policies;
- Prohibition of the sale of student data to private entities or organizations; and
- All personally identifiable student information being reported to the Department of Education or the Department of Enterprise Technology by a student's Wyoming student record identification and locator number as issued by the department of education.

If so, are there exceptions?

N/A

Data Minimization

Are there data retention limits?

There is no specific statute limiting how long data can/should be retained. However, the state superintendent is required to include data retention and disposition policies in their security plan.

Security

Is there a mandated data security program or specific security protocols?

TThere is no specific statute mandating a data security program or specific security protocols. However, physical and administrative safeguards such as data encryption and employee training are included in the Superintendent's data security plan.

Is there required de-identification or aggregation of data?

There is no specific statute requiring de-identification or aggregation of data.

Auditing and Accountability

Is there a requirement for a CPO for either school districts or companies receiving student data?

Wyoming does not appear to have codified a CPO requirement.

Is there a complaint process for student/parents when the law has been violated?

Wyoming does not appear to have codified such a complaint process.

Is there a private right of action?

Not specified by statute.

Individual Participation

Are parents/students able to opt-out of data collection or sharing?

Wyoming does not appear to have codified an ability to opt-out of data collection or sharing.

1401 K Street NW, Suite 200
Washington, D.C. 20005

202.637.9800

Questions?

*Reach out to our Privacy & Data team at **privacy@cdt.org**.*