Student Data Privacy, Accessibility, and Transparency Act

Summary

The Student Data Privacy, Accessibility, and Transparency Act (the "Act") requires the [State Board of Education/State Department of Education] to make publicly available on a continuing basis an inventory and index of the data elements with definitions of individual student data fields in the statewide longitudinal data system. The Act requires the [State Board of Education/State Department of Education] to create a data security plan to complement federal and state data privacy laws and policies governing the state longitudinal data system, and to provide student data privacy and security-related guidance to local education agencies. The Act grants authority to the [State Board of Education/State Department of Education] to establish policies for the protection of student data not only in the state's longitudinal data system, but also in data systems maintained by local educational agencies in the state. The Act requires certain third parties that receive student-generated content as a result of K-12 school purposes to implement certain security practices, and prohibit them from engaging in targeted advertising, selling student data, building profiles on students, or sharing student data except under limited circumstances. The Act creates a Chief Privacy Officer within the State Department of Education, whose primary responsibility would consist of ensuring department-wide compliance with all student data privacy and security laws and regulations. The Act also authorizes the Chief Privacy Officer to issue student data privacy and security policies applicable to local educational agencies and to handle appeals by parents regarding their rights under this Act. Finally, the Act adds new annual security and privacy reporting requirements to the Governor and Legislature.

Model Legislation

Section 1. {Title}

(A) This law shall be known and may be cited as the "Student Data Privacy, Accessibility and Transparency Act."

Section 2. {Legislative Intent}[i]

(A) The Legislature acknowledges that student data is a vital resource for parents, teachers, and school staff, and it is the intent of the Legislature to ensure that student data is safeguarded and that students' and parents' privacy is honored, respected, and protected. Student data allows parents and students to make more informed choices about educational programs and to better gauge a student's educational progress and needs. Teachers and school staff utilize student data in planning responsive education programs and services, scheduling students into appropriate classes and completing reports for educational agencies. Student information is critical in helping educators assist students in successfully graduating from high school and being ready to enter the workforce or postsecondary education. In emergencies, certain information should be readily available to school officials and emergency personnel to assist students and their families. A limited amount of this information makes up a student's permanent record or transcript. The Legislature firmly believes that student information is important for educational purposes, and it is also critically important to ensure that student information is protected, safeguarded, kept private, and used only by appropriate educational authorities to serve the best interests of the student. To that end, this law will help ensure that student information is protected and expectations of privacy are upheld.

Section 3. {Definitions}

(A) As used in this act:

(1) "Board" means the State Board of Education;

(2) "Department" means the State Department of Education;

(3) "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:

(i) the student's first and last name;

(ii) the name of the student's parent or other family members;

(iii) the physical address, email address, phone number, or other information that allows physical or online contact of the student or student's family;

(iv) a student's personal identifier, such as the student number, when used for identification purposes;

(v) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

(vi) state-, district-, school-, or teacher-administered assessment results, including participation information;

(vii) course transcript information including but not limited to courses taken and completed, course grades and grade point average, credits earned, degree, diploma, credential attainment, or other school exit information;

(viii) attendance and mobility information between and within [STATE] local education agencies;

(ix) the student's gender, race, and ethnicity;

(x) program participation information required by state or federal law;

(xi) disability status;

(xii) socioeconomic information;

(xiii) food purchases; or

(xiv) emails, text messages, documents, search activity, photos, voice recordings, and geolocation information.

(b) such information that:

(i) is created or provided by a student, or the student's parent or legal guardian, to an employee or agent of the school, local education agency, or state education agency or 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;

(ii) is created or provided by an employee or agent of the school or local education agency, including to an operator in the course of their use of the operator's site, service, or application for K-12 school purposes; or

(iii) is gathered by an operator through the operation an operator's site, service, or application for K-12 school purposes.

(4) "Education record" means an education record as defined[ii] in the Family Educational Rights and Privacy Act (FERPA) and its implementing regulations, 20 U.S.C. § 1232g; 34 CFR 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 or local education agency employees, nor does it include student data that a local education agency determines cannot reasonably be made available to the parent or eligible student;

(5) "Eligible student" means a student who has reached 18 years of age or is attending an institution of postsecondary education;

(6) ''Student personally identifiable data'' or "student personally identifiable information" or "personally identifiable information" means student data as defined in paragraph (3) that, alone or in combination, is linked to a specific student that would allow a reasonable person, who does not have personal knowledge of the relevant circumstances, to identify the student;

(7) "Aggregate student data" means data that is not personally identifiable and that is collected and/or reported at the group, cohort, or institutional level;

(8) "Provisional student data" means new student data proposed for inclusion in the state student data system;

(9) "Redacted data" or "de-identified data" means a student dataset that is not personally identifiable information because the educational agency or institution or other party has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information;

(10) "State-assigned student identifier " means the unique student identifier assigned by the state to each student that shall not be or include the Social Security number[iii] of a student in whole or in part;

(11) "State data system" means the State Department of Education statewide longitudinal data system;

(12) "K-12 school purposes" means purposes that take place at the direction of the K-12 school, teacher, or local education agency or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, preparing for postsecondary education or employment opportunities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school;

(13) "Operator" means any entity other than the department, local education agency, or school to the extent that the entity:

(a) Operates an Internet website, online service, online application, or mobile application with actual knowledge that the website, service, or application is used for K-12 school purposes and was designed and marketed for K-12 school purposes to the extent that it is operating in that capacity; and

(b) Collects, maintains, or uses student personally identifiable information in a digital or electronic format; and

(14) "Targeted advertising" means presenting advertisements to a student where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications, or student data. 'Targeted advertising' does not include advertising to a student at an online location based upon that student's current visit to that location or single search query without collection and retention of a student's online activities over time.

Section 4. {Chief Privacy Officer}

(A) The Superintendent shall appoint a Chief Privacy Officer, who shall report directly to, and be under the general supervision of, the Superintendent, to assume primary responsibility for data privacy and security policy, including:

(1) establishing department-wide policies necessary to assure that the use of technologies sustain, enhance, and do not erode, privacy protections relating to the use, collection, and disclosure of student data;

(2) ensuring that student data contained in the State Department of Education student data system is handled in full compliance with this Act, FERPA, and other state and federal data privacy and security laws;

(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of student data by the Department;

(4) conducting a privacy impact assessment on proposed legislative proposals, regulations, and program initiatives of the Department , including the type of personal information collected and the number of students affected;

(5) coordinating with the Office of the General Counsel and other legal entities as necessary to ensure that state programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner;

(6) preparing a report to the Legislature[iv] on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, internal controls, and other matters;

(7) working with the Department Chief Information Officer, General Counsel, and other officials in engaging with stakeholders about the quality, usefulness, openness, and privacy of data;

(8) establishing and operating a Department-wide Privacy Incident Response Program to ensure that incidents are properly reported, investigated, and mitigated, as appropriate;

(9) establishing and operating a process for parents to file complaints of privacy violations or inability to access their child's education records against the responsible local educational agency under Section 8 of this Act; and

(10) providing training, guidance, technical assistance, and outreach to build a culture of privacy protection, data security, and data practice transparency to students, parents, and the public among all state and local governmental education entities that collect, maintain, use, or share student data;

(B) The Chief Privacy Officer may investigate issues of compliance with this Act and with other state data privacy and security laws by the state educational agency and local educational agencies in the state and may:

(1) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the Chief Privacy Officer under this section;

(2) make such investigations and reports relating to the administration of the programs and operations of the Department as are necessary or desirable; and

(3) in matters relating to compliance with federal laws, refer the matter to the appropriate federal agency and cooperate with any investigations by such federal agency;

Section 5. {Data Inventory and Security}

(A) The [State Board of Education/State Department of Education] shall:

(1) Create, publish, and make publicly available a data inventory and dictionary or index of data elements with definitions of student personally identifiable data fields in the state student data system to include, but not be limited to:

(a) any student personally identifiable data required to be reported by state and federal education mandates;

(b) any student personally identifiable data which is included or has been proposed for inclusion in the student data system with a statement regarding the purpose or reason for the proposed collection; and

(c) any student data that the State Department of Education collects or maintains with no current identified purpose;

(2) Develop, publish, and make publicly available policies and procedures for the state data system to comply with this Act and other applicable state and federal data privacy and security laws, including the Federal Family Educational Rights and Privacy Act (FERPA). Such policies and procedures shall include, at a minimum:

(a) Restrictions on granting access to student data in the statewide longitudinal data system, except to the following:

(1) students and their parents, as provided by the collecting local education agency;

(2) the authorized administrators, teachers, and other school personnel of local education agencies, and the contractors or other authorized entities working on their behalf, that enroll students who are the subject of the data and who require such access to perform their assigned duties;

(3) the authorized staff of the State Department of Education, and the contractors or other authorized entities working on behalf of the Department, who require such access to perform their assigned duties as authorized by law or defined by interagency or other data-sharing agreements; and

(4) the authorized staff of other state agencies in the State of [State], including contractors or other authorized entities working on behalf of a state agency that require such access to perform their duties pursuant to an interagency agreement or other data sharing agreement;

(b) Prohibitions against publishing student data other than aggregate data or de-identified data in public reports; and

(c) Consistent with applicable law, criteria for the approval of research and data requests from state and local agencies, the State Legislature, those conducting research including on behalf of the Department, and the public that involve access to student personally identifiable information.

(3) Unless otherwise provided by law or approved by the [State Board of Education/State Department of Education], not transfer student personally identifiable data to any federal, state or local agency or other non-governmental organization, except for disclosures incident to the following actions:

(a) a student transferring to another school/local education agency in state or out of state or a school/local education agency seeking help with locating a transferred student;

(b) a student enrolls in an institution of higher education or training program;

(c) a student registering for or taking a state, national, or multistate assessment where such data is required to administer the assessment;

(d) a student voluntarily participating in a program for which such a data transfer is a condition or requirement of participation;

(e) the federal government requires the transfer of student data for a student classified as a "migrant" for related federal program purposes;

(f) a federal agency requires the student personally identifiable data to perform an audit, compliance review, or complaint investigation; or

(g) if the eligible student, student's parent, or legal guardian request such transfer.

(4) Develop a detailed data security plan for the state data system that includes:

(a) guidelines for authorizing access to the state data system and to student personally identifiable data including guidelines for authentication of authorized access;

(b) privacy and security audits;

(c) plans for responding to security breaches, including notifications, remediations, and related procedures;

(d) data retention and disposal policies;

(e) data security training and policies including technical, physical, and administrative safeguards;

(f) standards regarding the minimum number of students or information that must be included in a data set in order for the data to be considered aggregated and, therefore, not student personally identifiable data subject to requirements in this law and in other federal and state data privacy laws;

(g) a process for evaluating and updating as necessary the data security plan, at least on an annual basis, in order to identify and address any risks to the security of student personally identifiable data; and

(h) guidance for local education agencies to implement effective security practices that are consistent with those of the state data system;

(5) Ensure routine and ongoing compliance by the State Department of Education with FERPA, other relevant privacy laws and policies, and the privacy and security policies and procedures developed under the authority of this act, including the performance of compliance audits;

(6) Notify the Governor and the Legislature annually of the following matters relating to the state student data system:

(a) new student personally identifiable data proposed for inclusion in the state data system:

(1) any new provisional student data collection proposed by the Department shall become a provisional requirement to allow local education agencies and their local data system vendors the opportunity to meet the new requirement; and

(2) the [State Board of Education/Department of Education] must announce any new provisional student personally identifiable data collection to the general public for a review and comment period of at least 60 days;

(b) changes to existing student personally identifiable data collections required for any reason, including changes to federal reporting requirements made by the U.S. Department of Education;

(c) a list of any special approvals granted by the [State Board of Education/State Department of Education] under (A)(3) of this section in the past year regarding the release of student personally identifiable data, but such list need not include data shared pursuant to any of the exceptions listed in subsections (A)(3)(a) through (A)(3)(g) of this section;

(d) the results of any and all privacy compliance and security audits completed in the past year. Notifications regarding privacy compliance and security audits shall not include any information that would itself pose a security threat to the state or local student information systems or to the secure transmission of data between state and local systems by exposing vulnerabilities; and

(7) Develop policies and procedures to ensure the provision of at least annual notifications to eligible students and parents regarding student privacy rights under federal and state law.

Section 6. {Student Data Collection and Reporting Restrictions}

(A) Unless required by state or federal law or in cases of health or safety emergencies, local education agencies shall not report to the state the following individual student data or student information:

(1) juvenile delinquency records;

(2) criminal records;

(3) medical and health records; and

(4) student biometric information, unless a local education agency determines the information is necessary for educational purposes, such as for identification for online state assessment, provided the information is deleted when no longer needed for this purpose and not maintained as part of a student's permanent education record.

(B) Unless required by state or federal law or in cases of health or safety emergencies, schools shall not collect the following data on students or their families:

(1) political affiliation;

(2) voting history;

(3) income, except as required by law or where a local education agency determines income information is required to apply for, administer, research, or evaluate programs to assist students from low income families; or

(4) religious affiliation or beliefs.

Section 7. {Restrictions on Operators Use of Student Data}[v]

(A) An operator shall not knowingly engage in any of the following activities with respect to such operator's site, service, or application without explicit written or electronic consent from the student's parent or guardian, or an eligible student:

(1) (a) Use student data to engage in targeted advertising on the operator's site, service, or application, or (b) target advertising on any other site, service, or application when the targeting of the advertising is based upon any student data and state assigned student identifiers or other persistent unique identifiers that the operator has acquired because of the use of such operator's site, service, or application.

(2) Use information, including state-assigned student identifiers or other persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a student except in furtherance of K-12 school purposes. For purposes of this paragraph, 'amass a profile' does not include collection and retention of account records or information that remains under the control of the student, parent, or local education agency.

(3) Sell a student's data. This prohibition does not apply to the purchase, merger, or other type of acquisition of an operator by another entity, provided that the operator or successor entity continues to be subject to the provisions of this section with respect to previously acquired student data that is subject to this Act.

(4) Disclose student personally identifiable data without explicit written or electronic consent from a student over the age of 13 or a student's parent or guardian, given in response to clear and conspicuous notice of the activity, unless the disclosure is made:

(a) In furtherance of the K-12 school purposes of the site, service, or application; provided, however, that the recipient of the student data disclosed:

(i) Shall not further disclose the student data unless done to allow or improve operability and functionality within that student's classroom or school; and

(ii) Is legally required to comply with the requirements of this Act;

(b) To ensure legal or regulatory compliance or protect against liability;

(c) To respond to or participate in judicial process;

(d) To protect the security or integrity of the entity's website, service, or application

(e) To protect the safety of users or others or security of the site; or

(f) To a service provider, provided that the operator contractually (i) prohibits the service provider from using any student data for any purpose other than providing the contracted service to, or on behalf of, the operator, (ii) requires such service provider to impose the same restrictions as in this subsection on its own service providers, and (iii) requires the service provider to implement and maintain reasonable security procedures and practices as provided in subsection (B).

(B) An operator shall:

(1) 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.

(2) Delete a student's data within a reasonable timeframe not to exceed 45 days if the school or local education agency requests deletion of data under the control of the school or local education agency.

(C) Notwithstanding paragraph (4) of subsection (A), an operator may disclose student data, as long as paragraphs (1) to (3), inclusive, of subsection (A) are not violated, under the following circumstances:

(1) If another provision of federal or state law requires the operator to disclose the student data, and the operator complies with applicable requirements of federal and state law in protecting and disclosing that information.

(2) For legitimate research purposes: (a) as required by state or federal law and subject to the restrictions under applicable state and federal law or (b) as allowed by state or federal law and under the direction of a school, local education agency, or state department of education, subject to compliance with subsection A.

(3) To a state agency, local education agency, or school, for K-12 school purposes, as permitted by state or federal law.

(D) Nothing in this section prohibits an operator from using student data, including student personally identifiable data, as follows:

(1) For maintaining, delivering, developing, supporting, evaluating, improving, or diagnosing the operator's site, service, or application;

(2) Within other sites, services, or applications owned by the operator, and intended for the school or student use, to evaluate and improve educational products or services intended for the school or student use;

(3) For adaptive learning or customized student learning purposes;

(4) For recommendation engines to recommend additional content or services to students within a school service's site, service, or application without the response being determined in whole or in part by payment or other consideration from a third party;

(5) To respond to a student's request for information or for feedback without the information or response being determined in whole or in part by payment or other consideration from a third party; or

(6) To ensure legal or regulatory compliance or to retain such data for these purposes.

(E) Nothing in this section prohibits an operator from using or sharing aggregate data or de-identified data as follows:

(1) For the for the development and improvement of the operator's site, service, or application or other educational sites, services, or applications; or

(2) To demonstrate the effectiveness of the operator's products or services, including in their marketing.

(F) This section shall not be construed to limit the authority of a law enforcement agency to obtain any content or student data from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

(G) This section does not apply to general audience Internet websites, general audience online services, general audience online applications, or general audience mobile applications even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications.

(H) This section shall not be construed to limit Internet service providers from providing Internet connectivity to schools or students and their families.

(I) This section shall not be construed to prohibit an operator from marketing educational products directly to parents so long as the marketing did not result from the use of student data obtained without parental consent by the operator through the provision of services covered under this section.

(J) This section shall not be construed to impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance of this section on those applications or software.

(K) This section shall not be construed to impose a duty upon a provider of an interactive computer service, as defined in Section 230 of Title 47 of the United States Code, to review or enforce compliance with this section by third-party content providers.

(L) This section shall not be construed to impede the ability of a student or parent or guardian to download, transfer, or otherwise save or maintain their own student data or documents.

(M) Nothing in this section or this Act prevents a state or local education agency and their employees from recommending, directly or via a product or service, any educational materials, online content, services, or other products to any student or their family if the state or local education agency determines that such products will benefit the student and does not receive compensation for developing, enabling, or communicating such recommendations.

Section 8. {Parental request for information; complaints of violation}

(A) Parents have the right to inspect and review their child's education record maintained by the school or local education agency.

(B) Parents have the right to request from the school or local education agency student data included in their child's education record, including student data maintained by an operator, except when the local education agency determines that the requested data maintained by the operator cannot reasonably be made available to the parent.

(C) Local education agencies shall provide parents or guardians with an electronic copy of their child's education record upon request, unless the local education agency does not maintain a record in electronic format and reproducing the record in an electronic format would be unduly burdensome.

(D) A parent shall have the right to request corrections to inaccurate education records maintained by a school or local board of education. After receiving a request demonstrating any such inaccuracy, the school or local education agency that maintains the data shall correct the inaccuracy and confirm such correction to the parent within a reasonable amount of time.

(E) The rights granted to parents in (A) through (D) of this section shall extend to eligible students seeking to access their own education records.

(F) The State Department of Education shall develop model policies for local education agencies that:

(1) support local education agencies in fulfilling their responsibility to annually notify parents of their right to request student information;

(2) assist local education agencies with ensuring security when providing student data to parents;

(3) provide guidance and best practices to local education agencies in order to ensure that local education agencies provide student data only to authorized individuals;

(4) support local education agencies in their responsibility to produce education records and student data included in such education records to parents and eligible students, ideally within three[vi] business days of the request; and

(5) assist schools and local education agencies with implementing technologies and programs that allow parents to view online, download, and transmit data specific to their child's education record.

(G) The Chief Privacy Officer shall develop policies and procedures for parents or eligible students to file a complaint with the state or local educational agency regarding a possible violation of rights under this Act or under other federal or state student data privacy and security laws.

(1) Parents or eligible students not satisfied with the state or local agency's resolution of the matter may file an appeal with the Chief Privacy Officer.

(2) The Chief Privacy Officer shall establish a process for receiving and responding to such appeals pursuant to Section 4(A)(9).

(3) The Chief Privacy Officer, in response to an appeal:

(a) may dismiss a complaint before taking any other action if the complaint fails to allege any violation of this Act [*referring to the entire Act*];

(b) may investigate the allegations in the complaint pursuant to the investigatory authority granted by Section 4(B) of this Act;

(c) shall, if the complaint is not dismissed, issue a written advisory opinion within 30 calendar days, unless extraordinary circumstances justify an extension of time, after the complaint is filed concerning whether or not a violation of the parent's or student's rights occurred, which shall be available to the public except for those portions which could reveal the identity of a student or a parent; and

(d) shall refer any possible violations of federal law to the appropriate federal agency or agencies for further investigation.

(H) Nothing in this section authorizes any additional cause of action beyond the process described in this section or as otherwise authorized by state law.

Section 9. {Rules}

(A) The [State Board of Education/State Department of Education] may adopt rules necessary to implement the provisions of this Act.

(B) Upon the effective date of this Act, any existing collection of student data by the State Department of Education shall not be considered a new student data collection in accordance with subsection 3(A)(6) of this Act.

Section 10. {Effective Date} This Act shall become effective July 1, [20XX]. However, to the extent any provision of this Act conflicts with a term of a contract in effect before July 1, [20XX], such provision shall not apply to the state agency, local education agency, or the operator subject to such agreement until the expiration, amendment, or renewal of that agreement.

Explanatory Notes

[i] Language adapted from Idaho's "Student Data Accessibility, Transparency and Accountability Act of 2014," available at http://www.legislature.idaho.gov/legislation/2014/S1372E1.pdf.

[ii] FERPA defines "education records" broadly 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. (*See* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/students.html.)

Education records.
(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.
b) The term does not include:
(1) Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.
(2) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of §99.8.
(3)
(i) Records relating to an individual who is employed by an educational agency or institution, that:
(A) Are made and maintained in the normal course of business;
(B) Relate exclusively to the individual in that individual's capacity as an employee; and
(C) Are not available for use for any other purpose.
(ii) Records relating to an individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (b)(3)(i) of this definition.
(4) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:
(i) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;
(ii) Made, maintained, or used only in connection with treatment of the student; and
(iii) Disclosed only to individuals providing the treatment. For the purpose of this definition, "treatment" does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution; and
(5) Records created or received by an educational agency or institution after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student.
(6) Grades on peer-graded papers before they are collected and recorded by a teacher.
(Authority: 20 U.S.C. 1232g(a)(4))

[iii] Some states' workforce data systems use Social Security numbers for unemployment purposes. Policymakers in these states should consider how to link their states' workforce and education data while also maintaining the highest standards of privacy and security.

[iv] The chief privacy officer could submit the report to the legislature directly, the report could come from the state superintendent, or it could be a joint submission, depending on the state's governance structure.

[v] These provisions were adapted from California's Assembly Bill 1177 (2014), available at http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_1151-1200/sb_1177_bill_20140828_enrolled.htm.

[vi] Policymakers might choose a timeframe shorter or longer than three days. FERPA currently requires the production of education records within 45 days, (34 C.F.R. § 99.10(b)), which is not sufficient for informing parents of their child's current educational progress, for providing them with timely information upon which to base decisions, or for helping parents identify any additional educational services their child might need.