Data Privacy and Security Considerations

Using and sharing students' educational records is vital to understanding what is working and what needs improvement in the field of early learning. This use and sharing is encouraged for professional learning and continuous improvement in preparing children for success in school and life. At the same time, these educational records often contain sensitive personally identifying information about the student that is protected from disclosure under state and federal laws. Accordingly, student privacy and data security must be at the forefront of all aspects of data sharing.

Typically, sharing data requires consent by the child's parent or guardian. However, federal laws permit disclosure without consent under certain circumstances. Moreover, educational institutions that have received funding by the U.S. Department of Education may release de-identified education records without obtaining consent by the parents. To do so, all personally identifiable information must be removed and the educational institution must make a reasonable determination that a student's identity cannot be determined by the remaining information, together with other reasonably available information.

Abiding by the laws that govern data privacy should be viewed as the minimum users should do. Users should seek to further protect student privacy whenever possible as they work together to continuously improve programs and practices. The following set of guidelines is intended to give data users a basic understanding of the laws and practices to keep in mind as they collaborate in creating better outcomes for children.

Applicable Federal Laws

Parties should ensure that their data privacy and security practices comply with applicable laws. These include, but are not limited to, federal laws such as the Family Educational Rights and Privacy Act ("FERPA"), the Protection of Pupil Rights Amendment ("PPRA"), and the Children's Online Privacy Protection Act ("COPPA") Rule. In addition, parties should comply with applicable Indiana law.

Privacy and Security Principles

In addition to following applicable laws, the following general privacy and security principles should be taken into account:

1. ***Governance.*** Parties should define, document, communicate and assign accountability for their privacy and security policies and procedures.

2. ***Collection Limitation.*** There should be limits to the collection of personally identifiable information. Generally, entities should not collect data they do not plan to use. Any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

3. ***Data Quality.*** Personally identifiable information should be relevant to the purposes for which it is to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

4. ***Purpose Specification (Notice).*** The purposes for which personally identifiable information is collected should be specified not later than at the time of data collection. Later use should be limited to the fulfillment of those purposes or other compatible purposes as are specified on each occasion of change of purpose.

5. ***Use Limitation.*** Personally identifiable information should be used only in accordance with the specified purpose or notice given, except (a) with the consent of the data subject; or (b) by the authority of law.

6. ***Retention and Disposal.*** Parties should keep personally identifiable information for only as long as necessary to fulfill the stated purposes or as required by law. Thereafter, parties should appropriately dispose of the information.

7. ***Security Safeguards.*** Personally identifiable information should be protected by reasonable security safeguards (e.g. encryption, network segmentation, data transmission guidelines) against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

8. ***Transparency.*** Where appropriate and without compromising the data security, there should be a general policy of transparency about developments, practices and policies with respect to personally identifiable information. Generally, it should be easy for parents and students to find out what data is being collected and for what purpose.

9. ***Individual Participation.*** Where required by law or otherwise appropriate, individuals should be provided the ability to know whether or not the party controlling the data has data relating to them. Generally, it should be easy for parents and students to find out who is holding their data.

10. ***Accountability.*** Any third parties to whom data is disclosed should be accountable for complying with these principles. Further, the party who collected the data should monitor compliance with its privacy and security policies and procedures. The party should also have procedures to address complaints and disputes.

Frequently Asked Questions (FAQ)

For guidance to those involved in the early learning data system, here are some frequently asked questions and answers on student privacy:

What is FERPA?

FERPA is a federal law that protects the privacy of student education records. Generally, FERPA affords parents the right to request and control the disclosure and use of their children's education records. In addition, FERPA provides that schools may not disclose students' education records to third parties without parental consent or consent of an eligible student unless under specific circumstances. FERPA applies to all schools, educational agencies, or institutions that receive funds under an applicable program of the U.S. Department of Education.

Am I allowed to share student information with third parties if I don't have consent?

Yes, under limited circumstances. FERPA names several exceptions to the consent requirement. Two common exceptions are the "studies exception" and the "audit exception." Under these exceptions, a student's Personally Identifiable Information from education records may be disclosed without consent if the third party and school executed a written agreement regarding the disclosure. FERPA mandates that certain terms be included in the agreements, depending on whether it is for an audit or survey. The Department of Education has compiled the required terms in a user-friendly guideline titled "Guidance for Reasonable
Methods and Written Agreements," which is available at
http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf.

What constitutes Personally Identifiable Information?

Personally identifiable information is any information that reasonably identifies a student. This includes a student's or parent's first and last name, a home or other physical address (including a street name and the name of a city or town), a telephone number, a social security number, student's or parent's dates of birth, places of birth, or mother's maiden name.

Can I or my school redact or remove Personally Identifiable Information and then disclose information in an education record?

This process is called "de-identifying" records. Records and information are de-identified once all Personally Identifiable Information has been removed, including, but not limited to any information that, alone or in combination can be linked to a specific student that a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, can identify the student with reasonable certainty. Schools may release de-identified education records without the consent required by FERPA if all Personally Identifiable Information has been removed from the record and the school has made a reasonable determination that a student's identity cannot be determined by the remaining information, taking into account other reasonably available information.

What is "PPRA"? Does it apply to my school?

The Protection of Pupil Rights Amendment ("PPRA") is another federal law that applies to schools and institutions that receive funding from the U.S. Department of Education. PPRA governs the administration of surveys, analyses, or evaluations to students which are funded by the Department of Education. PPRA seeks to ensure that schools make

instructional materials available for inspection by parents if those materials will be used in connection with the survey.

Moreover, PPRA requires parental consent when a study or evaluation seeks identifying information regarding eight enumerated subject matters: (1) political affiliations; (2) mental and psychological problems; (3) sex behavior and attitudes; (4) illegal, anti-social, self-incriminating and 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); income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program); and (8) religion.

If I comply with FERPA, can I still be sued?
Yes. FERPA is a floor and not a ceiling to the protection schools must afford to students' records. FERPA and its regulations merely form the baseline of required protections. As such, the Department of Education has issued best practices that are broader than FERPA. Some of these practices include encrypting student data, disclosing only the minimum information that is needed, and having a data breach response plan that includes notifying counsel within ten days of a breach.

Sources and Other References

FERPA: 20 U.S.C. § 1232h; 34 CFR Part 98
PPRA: 20 U.S.C. § 1232g; 34 CFR Part 99
COPPA: 15 U.S.C. § 6501, *et seq.*; 16 C.F.R. Part 312
Indiana Parental Access to Education Records, Ind. Code § 20-33-7-1, *et seq.*
Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9-1, *et seq.*
Indiana Special Education regulations, 511 IAC 7-32 through 7-47
Indiana Notice of Security Breach Act, Ind. Code § 4-1-11, *et seq.*
Department of Education FERPA website, *available at* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
FERPA Frequently Asked Questions, answered by the Department of Education, *available at* https://www2.ed.gov/policy/gen/guid/fpco/pdf/ferpafaq.pdf.
FERPA Frequently Asked Questions, answered by the Family Policy Compliance Office, available at http://familypolicy.ed.gov/faq-page.
Department of Education PPRA website, *available at* http://www2.ed.gov/policy/gen/fuid/fpco/ppra/index.html.
Complying with COPPA: Frequently Asked Questions, answered by the Federal Trade Commission, *available at* http://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools.
Office of the Public Access Counselor, www.in.gov/pac.
December 2014 Department of Education Superintendent Notice, *available at* http://www2.ed.gov/policy/gen/guid/fpco/pdf/superint-notice.pdf.

Department of Education, *The Family Educational Rights and Privacy Act Guidance for Reasonable Methods and Written Agreements*, pgs. 5-9, http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf.
Department of Education, *Model Notification of Rights Under the Protection of Pupil Rights Amendment (PPRA*), *available at* http://www2.ed.gov/policy/gen/guid/fpco/doc/ppra-gen-not.doc.
Peter P. Swire & Kenesa Ahmad, *Foundations of Information Privacy and Data Protection: A Survey of Global Concepts, Laws and Practices* (2012). *See also Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Sept. 23, 1980, Organisation for Economic Co-operation and Development; AICPA/CICA Privacy Task Force, *Generally Accepted Privacy Principles* (GAPP), *available at* http://www.aicpa.org/interestareas/informationtechnology/resources/privacy/generallyacceptedprivacyprinciples/pages/default.aspx

I\6584364.1