DATA PRIVACY AND SECURITY

Working Group Report: November 2014

Background and Process of the Working Group

During the spring 2014 legislative session, two bills were filed, HB 4558 (Drury) and SB 3092 (Delgado) that addressed student data privacy. During discussions held with the sponsors of these bills, education stakeholder groups, including those from early learning, k-12 and higher education, expressed concerns about the language of the proposed legislation. In consideration of these concerns, the bills were held with the expectation that discussions on student data privacy would continue during the summer.

To meet that commitment, the Illinois State Board of Education (ISBE) and the P-20 Council sponsored an initial meeting, held on June 25th, to which all groups that had been involved in the discussions during the legislative session were invited, along with the sponsors. The goals of the meeting were to re-familiarize everyone with the existing laws on student data privacy, discuss work in other states and at the federal level on this topic, discuss the uses of data in education and to identify areas of concern to be addressed in future legislation. The agenda for the June 25th meeting is attached as Exhibit A.

At the conclusion of the meeting, the group agreed to convene a smaller working group to review all of the issues raised, to research the issues and to come back to the larger group with recommendations. A list of the participants in the working group is attached as Exhibit B. The working group held three meetings over the summer and fall.

Prior to the first working group meeting held on July 21st, participants were asked to answer some key questions about concerns about data use and data privacy. This questionnaire is attached as Exhibit C, along with the answers received. Building on the information submitted, the group had in depth discussion during its July 21st meeting about the various issues surrounding student data privacy in attempt to categorize and prioritize the issues. The notes from that meeting are attached as Exhibit D. It was decided at the end of the July 21st meeting that each participant would go back to the stakeholders they represented and identify use case examples. The use case examples submitted are compiled in Exhibit E.

During the second meeting on September 8th, the group broke into smaller groups and discussed all the use case examples. Ultimately, the group decided that it would be most helpful to organize the use cases on a chart that identified whether the use case required the use of identified student data, de-identified student data or aggregate data. The chart is reproduced in the body of this report at pages 4-7 and is discussed therein.

The final meeting of the working group was held on October 21st and included a review of this report and a decision on the recommendations that would be made herein to the larger group. In addition, the group discussed timelines for forthcoming legislation based on use cases.

Data Use

Education data have a wide variety of uses critical to the efficient and effective provision of educational services. These uses include providing access to curricular and assessment materials, developing evidence for improving schools and instruction, effectively running schools (including everything from ensuring transportation needs are met to running the cafeteria), and ensuring communication and collaboration between education providers from early learning through higher education. Education data can empower educators, students, parents and policy makers with the information that they need to make the best decisions to improve the quality of education in Illinois. Among other uses, data can help teachers personalize learning and create dynamic classroom environments; empower parents and the public to hold schools accountable for student and teacher performance; and help ensure that tax dollars are being used effectively.

A central component to the use of data in education is ensuring that data are being collected for meaningful purposes and that data are being kept safe, secure and private. Also central is the need to communicate effectively and clearly with students, parents and the general public about the use of data, the value in collecting data and the safeguards in place that ensure data privacy. Only through acknowledging and ensuring that both of these components are met will educators and policy makers build trust and support around the use of student data.

The key charge and challenge for Illinois is to ensure that robust data use is protected and valued while simultaneously ensuring that data are secure.

Because data security is critical, this working group recommends a number of approaches to ensuring that education data is appropriately safeguarded, including legislation, guidance and model documents. The recommendations are laid out in more detail on pages 9 and 10 of this report. While recognizing that it is impossible to provide absolute security for data, the group believes that by creating high-quality policies and practices that govern data protection and use, we can engage all stakeholders in a culture of valuing data, clearly communicating about data and understanding and practicing proper data use.

Concerns:

The working group identified a number of concerns with data collection and use:

- Third-party vendors and research organizations have access to data but it is not clear that districts are consistent when negotiating for what purposes those vendors are using the data and how the data is being protected.
- There is a lack of transparency on data use and data sharing, leaving parents and students and teachers without a full understanding of why data is being collected, by whom and for what purpose.

Districts have a varying level of capacity to ensure that they are in compliance with state and federal laws covering data use and sharing, that they have appropriate data sharing agreements in place, that their physical data storage is secure and that they have protection against data breach.

Longitudinal Data System Governance

The State of Illinois is now actively moving forward with the design and development of the state-wide Illinois Longitudinal Data System (ILDS). The system, when fully deployed, will provide data to help to track the outcomes of Illinois students as they progress from early learning through Postsecondary education, and as they enter the workforce. Longitudinal data supports an in-depth, comprehensive view of students' progress and will ultimately help guide policymakers on where to invest time and energy to most effectively improve student achievement in our State.

The ILDS is defined by Public Act 96-0107 and enabled through federal funding, and instructs the State Board of Education to link student test scores, length of enrollment and graduation records over time. The system also will connect students to career planning and resources, with the potential to facilitate the application process for financial aid and records for transfer students.

On June 30, 2013, seven State of Illinois agencies[1] and the Office of the Governor entered into a landmark intergovernmental agreement for the governance of the Illinois Longitudinal Data System ("LDS"). This Agreement identified eight separate requirements, functions, and expectations for the focus of the LDS governance system (the "LDS Functions"). In addition, the Agreement created (i) a Governing Board with senior leadership from each of the LDS Agencies and chaired by an appointee of the Governor, and (ii) five separate committees. The focus of the LDS Governance System are the following: (1) Ensure robust protections for individual privacy

[1] The seven agencies are: Illinois Board of Higher Education (IBHE), Illinois Community College Board (ICCB), Illinois Department of Commerce and Economic Opportunity (DCEO), Illinois Department of Employment Security (IDES), Illinois Department of Human Services (IDHS), Illinois Student Assistance Commission (ISAC), Illinois State Board of Education (ISBE)

and compliance with all pertinent state and federal laws; (2) Establish a set of tools, systems, and processes internal to LDS Agencies and shared across LDS Agencies to meet the expectations and requirements of the P-20 Longitudinal Education Data System Act and support analysis and understanding of lifelong education and workforce policies and programs; (3) Effectively and efficiently address audit, evaluation, and research needs that require data inputs from multiple LDS Agencies; (4) Support and advance sound, research-based decision-making within the LDS Agencies and for all State education and workforce policymakers; (5) Effectively address common issues across LDS Agencies such as data access, use, and security; (6) Establish the expectation that LDS Agencies share data in accordance with established procedures and protocols, subject to applicable legal restrictions; (7)Develop a common process across the LDS Agencies to plan and budget for LDS implementation, improvement, and maintenance; and (8) Effectively utilize knowledge and expertise relating to the LDS Functions residing at the LDS Agencies and capitalize on a cost-effective LDS Agency distributed data system model that avoids duplication and ensures sustainability.

Use Cases

In an effort to identify the potential impact of various approaches to policy and practice recommendations, the working group spent time compiling and analyzing various uses of data by the early childhood community, k-12 districts and higher education. Further, the group identified in which cases the use of identifiable data needed to be shared, in which cases de-indentified data could be use and where aggregate data was all that was needed. The goal of this analysis was to get a handle on when and where we are using data and to assist with highlighting those uses of data where we believe we need to focus our attention on safety and security. The following chart is a compilation of this analysis. It is important to note that this chart is not meant to be exhaustive in terms of uses of data but rather examples are given to be illustrative of the types of data used by each user.

Framework for Analyzing Key Privacy and Security Concerns

User[i]	Identifiable Data[ii]	De-Identified Data[iii]	Aggregated Data[iv]
State agencies	• ISBE contracts with assessment vendor to administer and report on state assessment. • ISBE collects data on students through its SIS to enable program evaluation, public reporting and creation of legislatively and federally mandated	• N/A	• ISBE collects aggregate data on a number of topics that are too sensitive for state-level individual collection (e.g., immunizations, dental health)

User[i]	Identifiable Data[ii]	De-Identified Data[iii]	Aggregated Data[iv]
	reporting.		
School districts	• District creates its own internal student information system to track student progress and growth.	• Link program and teacher characteristics to longitudinal child data.	• Survey conducted to obtain stakeholder opinions and feedback, including those from students.
School district vendors/contractors[v]	• District contracts with a food service provider to administer its lunch program. (The Point of Sale system may be contracted to a "fourth party" to electronically process transactions.) • District contracts with third party to host web-based student information system. • District contracts with third party to host a web-based instructional information system. • Districts contract with individual education technology vendors to provide on-line educational programming for classrooms and homework. • Districts contract with technology vendors to provide students with devices and web-based tools (e.g. ipads and gmail accounts). • District contracts with assessment vendor to acquire assessment and to process assessment data. • Districts utilize web-based applications and	• Contracted research on district programs and policies	• Contracted research on district programs and policies

User[i]	Identifiable Data[ii]	De-Identified Data[iii]	Aggregated Data[iv]
	services to provide basic communication and collaboration services.		
Service provider partners[vi]	• Share assessment data between kindergarten teachers and community-based preschool teachers.	• Identify school outcomes (daily attendance, grades, 3rd grade test scores, special education supports) for children who have used different types of ECE.	
Parents and Students	• Student and parents review student records to ensure accuracy.	•	Review aggregate data on Illinois School Report Card to compare schools and districts
Teachers and Other Educators	• Review and analyze data of students to ascertain performance of individual students. • Review data on their students to ensure accuracy.	• Access and analyze data for program, school and district improvement. • Access data to look for trends and patterns in students.	• Review data to better understand school, district and state context for their own students.
Researchers	• Researchers evaluate policies/practices in schools with existing student and teacher data using data from a single agency or multiple agencies with appropriate data sharing agreements.	• Same as identifiable data, but no identifying information or a scrambled identifier to match records across datasets is used. This is the most common form of data sharing with researchers	• Same as identifiable data, but data are aggregated.
3rd Party Requesters (e.g. advocates, legislature, reporters, general public, FOIA requests)	• N/A	• Provide summary reports about schools and districts about trends and patterns in student performance. Data are redacted when cell size is <10 to ensure anonymity of students/teachers	• Same as de-identified data, but reported in aggregate.

[ii] This column identifies categories of users, with the expectation that linkages across these categories – and within them – will be necessary to address certain important use cases.

[ii] Because of the varying uses of identifiable data, this column will require the most attention for developing privacy and security protections.

[iii] Providing de-identified data will require a focus on the privacy and security requirements of the process for de-identifying the data. Once the data has been de-identified (by the holder(s) of the data or others), the use of the de-identified data will pose fewer data and security concerns. Note that most of the uses in this column are closely related to uses for which individually identifiable data is necessary, and that individually identifiable data could be used to answer the questions in this column even though it is not necessary that the data be individually identifiable.

[iv] Providing aggregated data will require a focus on the privacy and security requirements of the process for aggregating the data. Once the data has been aggregated (by the holder(s) of the data or others), the use of the aggregated data will pose fewer data and security concerns.

[v] This category will include numerous different kinds of contractors, such as testing contractors or food service contractors. Each of these may raise their own privacy and security concerns depending on the particular uses.

[vi] This category will include numerous different kinds of providers, including community-based preschools and health providers. These organizations will in many instances seek to share individual data with schools (and each other) as part of their service delivery to children.

Other States

The working group looked at other states to identify key pieces of legislation that could serve as models for Illinois.

In 2014, in 36 of the 46 states that held legislative sessions in 2014 there were bills introduced on student data privacy. During the 2014 session, 110 bills regarding safeguarding student data were considered by these states and 30 data privacy bills were passed by 21 states.

The working group specifically focused its attention on the two bills passed in California and the legislation passed in Idaho. These laws can be found at the following citations:

California:
https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB1177

http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201320140AB1584&search_keywords=school+contract

Idaho: http://legislature.idaho.gov/legislation/2014/S1372E1.pdf

The working group also plans to create a cross-walk of state legislation to review and compare relevant legislative provisions to better inform the drafting of Illinois legislation. That crosswalk will be provided as an addendum to this report when completed.

Recommendations

The purpose of the Framework for Analyzing Key Privacy and Security Concerns is to inform any legislation, guidance, or model documents – so that the privacy and security protections adopted for a particular kind of data use are appropriate for that kind of data use. Because different users and types of data use raise different privacy and security concerns, the framework is meant to inform privacy and security protections that allow for appropriate data use while still safeguarding protected data. In particular, individually identifiable data raises special concerns that will need to be addressed in a manner distinct from the protections on aggregated or de-identified data, and different kinds of individually identifiable data will each raise unique privacy and security issues

Legislation:

- Research Provisions: Amendments to ISSRA that would establish required procedures to be used when data is shared for research purposes. This legislation would build on Amendment 1 to HB 4558 from spring 2014 session which was substantially agreed to by all parties but which will be reviewed for small changes and refinements. The working group recommends that higher education stakeholders and Representative Drury work together to refine the language of the Amendment.
- District Provisions:
    - A strong statement of legislative intent that acknowledges the value of the effective use of data and the importance of establishing privacy and security safeguards to protect personally identifiable information of students, teachers and school personnel.
    - Notice to parents – the legislation should enhance the notification to parents about what data is collected at the district level and the purposes for the data collection.
    - Third-party vendors – the legislation requires that a district have a contract with a third-party vendor for data sharing and the legislation will specify required terms of these contracts, including use of the data, breach notification and mitigation procedures, administrative, technical and physical safeguards, storage and security protocols including data return and destruction, and training of employees.
    - Third-party vendors – restrictions on what third-party vendors can and cannot do with data, including the use of data for commercial purposes.
    - Teacher data – restrictions on the release of certain teacher data beyond current protections allowed by state and federal law.

Guidance:

- District Technology Policies: The group recommends that the State Board of Education, in collaboration with stakeholders, create guidance on the governance within districts of the use of data, including who within the district can make decisions on the online educational tools to be used in classrooms. This guidance would specifically address the district requirements to develop a policy regarding access of free online resources by

parents and teachers and would address the ability of teachers to agree to shrink wrap end user license agreements to access free on-line resources.

Model Documents:

- Data Share Agreement, Third-Party Vendors: The group recommends that the State Board of Education create a model data share agreement that can be used by school districts when contracting with third-party vendors. The model document should contain all the necessary provisions to comply with FERPA/ISSRA and should include a menu of provisions that can be swapped in and out depending on the nature of the contract and the data sharing involved. Districts will be cautioned to have district counsel review the data share agreement prior to execution.
- Data Share Agreement, Research: The group recommends that the State Board of Education create a model data share agreement that can be used by school districts when contracting with research entities.
- Parent Notice: While districts currently provide a "FERPA" notice to parents at the beginning of the school year, it is often lengthy and difficult to understand. The State Board of Education, in collaboration with stakeholders, will create a model notice to parents that clearly identifies what data are collected on each student in the district and for what purposes.

Training:

- Create training for district personnel (and others as needed) on data privacy, including the proper use of data, the limits of personnel to access and review data, and district policies regarding the use of data.

While beyond the scope of this report and focus of this group, the working group recognizes that the State needs to continue to work on ensuring that K-12 districts throughout the state have access to technology and technology infrastructure.