Unifying Student Data Privacy with Data Interoperability

~ the Unity Blueprint ~
Agenda

**Risks**
How do we decrease the risk of data “leakage” when so much data is flying around our digital ecosystem?

**Requirements**
How do you convey privacy legal requirements to marketplace providers?

**Standards**
Is there a way I can address/enforce privacy requirements through openly developed technical standards?

**Implementation**
How are your vendors implementing privacy requirements in the real world?

“Next”?
Who are we?

Steve Smith
CIO
Cambridge Public Schools, MA
ssmith@cpsd.us

Ben Silberglitt
CSO
Cedar Labs
Ben.Silberglitt@cedarlabs.com

Jeff Simons
CIO
WSIPC
jsimons@wsipc.org

John Lovell
Technology Director
A4L Community
jlovell@A4L.org
Level Setting.....

**Access 4 Learning Community**

- Non-Profit started in 1997
- Membership driven with schools, districts, regional and state agencies, other professional organizations and marketplace providers in the Community
- Collaboratively develops technical blueprints (SIF) for data to move safely and securely between school software applications
- Used in every state and Communities in 4 Countries
- [https://www.A4L.org](https://www.A4L.org)

**Student Data Privacy Consortium**

- Special Interest Group of A4L Community started in 2015
- Maintains its own governance, oversight and resource support
- 31 State Alliances representing over 9,000 schools and 75+ vendors
- Addressing privacy “Pain Points”
- Working collaboratively on projects, tools, effective practices and partnerships for “tactical student data privacy”
- [https://sdpc.A4L.org](https://sdpc.A4L.org)
How do we decrease the risk of data “leakage” when so much data is flying around our digital ecosystem?

Don’t worry, we are here to help you modernize your environment....
Its Not “One or the Other”!

No One Gets It!

Everyone Gets It!
A4L & SDPC: Supporting the “New School” Role?

• Increased interoperability without the inclusion of privacy requirements equals increased **RISK**.

• **BOTH** data sharing and privacy parameters must be identified and communicated.

• Learning institutions often do not have the human and/or fiscal resources to successfully address both parameters.

• A4L and SDPC is the **ONLY** community collaboration that is addressing **BOTH** interoperability and privacy.

“The A4L and SDPC Communities will help schools and marketplace providers establish “connected, secure and effective K12 ecosystems”

“Leadership and learning are indispensable to each other.”

John F. Kennedy
How do you convey privacy legal requirements to the marketplace providers?

…Clauses, Obligations, & Benchmarks, Oh My!
Linkages for Privacy.....

**Agreement CLAUSES**

**Main FERPA Exception:**
School officials with legitimate educational interest – a data privacy agreement is a must!

**National Data Privacy Agreement:** Standardize the DPA Format so it looks the same by identifying common legal clauses across jurisdictions

**Example:** "Upon written request from the LEA, Provider shall dispose of or provide mechanism for the LEA to transfer Student Data…” (IV, 6)

---

**Technical OBLIGATIONS**

How product providers will technically implement the agreement CLAUSES to adhere to customer requirements

Addressing the “legalese” of the CLAUSES to “technical effective practices”.

**Example:** “Acknowledge and register adequate signals for for the interpretation, operational execution and notice of deletion request”

---

**Standards BENCHMARKS**

Technical Standards establishing agreed principles or criteria so that their users can make reliable assumptions about technical OBLIGATIONS.

A technical standard is an established norm or requirement in regard to technical systems.

**Example:** “Execute delete requests and subsequent notice (to controller and/or subject) under reasonable timeframes and in accordance to retention schedules defined by purpose in the Service Agreement.” (NIST)
# National Data Privacy Agreement (NDPA) v1

<table>
<thead>
<tr>
<th>NDPA Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Format</strong></td>
<td>Designed to provide everything the reader needs to know on page 2</td>
</tr>
<tr>
<td>Section</td>
<td>Cover Page and Directive</td>
</tr>
<tr>
<td>Section</td>
<td>Page 2 - Options</td>
</tr>
<tr>
<td>Section</td>
<td>Page 3 - Signatories</td>
</tr>
<tr>
<td>Section</td>
<td>Standard Clauses</td>
</tr>
<tr>
<td>Section</td>
<td>- Exhibits</td>
</tr>
<tr>
<td></td>
<td>- A = Descriptions of Services</td>
</tr>
<tr>
<td></td>
<td>- B = Schedule of Data</td>
</tr>
<tr>
<td></td>
<td>- C = Definitions</td>
</tr>
<tr>
<td></td>
<td>- D = Directive for Disposition of Data</td>
</tr>
<tr>
<td></td>
<td>- E = General Offer of Terms</td>
</tr>
<tr>
<td></td>
<td>- F = Data Security Requirements</td>
</tr>
<tr>
<td></td>
<td>- G = Supplemental State Terms</td>
</tr>
<tr>
<td></td>
<td>- H = Additional Terms or Modifications</td>
</tr>
</tbody>
</table>
Is there a way I can address and enforce privacy requirements through openly developed technical standards?

Yes!
Linkages for Privacy…..

**Agreement CLAUSES**

Main FERPA Exception: School officials with legitimate educational interest – a data privacy agreement is a must!

**National Data Privacy Agreement:** Standardize the DPA Format so it looks the same by identifying common legal clauses across jurisdictions

**Example:** "Upon written request from the LEA, Provider shall dispose of or provide mechanism for the LEA to transfer Student Data…” (IV, 6)

---

**Technical OBLIGATIONS**

How product providers will technically implement the agreement **CLAUSES** to adhere to customer requirements

Addressing the “legalese” of the **CLAUSES** to “technical effective practices”.

**Example:** “Acknowledge and register adequate signals for for the interpretation, operational execution and notice of deletion request”

---

**Standards BENCHMARKS**

Technical Standards establishing agreed principles or criteria so that their users can make reliable assumptions about technical **OBLIGATIONS**.

A technical standard is an established norm or requirement in regard to technical systems.

**Example:** “Execute delete requests and subsequent notice (to controller and/or subject) under reasonable timeframes and in accordance to retention schedules defined by purpose in the Service Agreement.” (NIST)
<table>
<thead>
<tr>
<th>Clause</th>
<th>Obligation/Benchmark</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Destination of Data. Provider shall destroy or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transferred and data to USA or USA's designee, according to the procedure identified in Article II, Section 5 above. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maintain an accessible practice of destruction of data with adequate reference to definitions and policies in presenting general data retention guidelines.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Present a data retention policy which identifies data classifications, retention schedule, and destruction process in line with data classification level.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Property address and agree to the definition of delete (text: e.g., making unrecognizable, discuss extent such as backups/etc).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Acknowledge and register adequate signals for the interpretation, operational execution, and notice of deletion requests.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destroy data as a result of a delete request in accordance with Service Agreement... at end of service, if not of purposes use when no longer retained, when unlawfully collected or requested under local directive, where guardian has objected, where District is not clear controller of subject data, or where Parental consent has not been obtained for under 14</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Execute delete requests and subsequent notice (to controller and/or subject) under reasonable timeframes and in accordance with timeframes defined by purpose in the Service Agreement.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Identify which data or data types are to be retained, destroyed, and anonymized during deletion requests.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Demonstrate evidence of the execution of a delete request process at a data subject level while maintaining compliance.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recognize and plan for limits of data destruction.</td>
<td></td>
</tr>
</tbody>
</table>

**Alignment to Known Standards**

**NIST 800-53 (Rev. 4) System and Information Integrity Control Family SI-12 Information Handling and Retention.**

National retention standards can be found here:


for specific local standards (state, provinces, territory) see the local department responsible for data retention schedules.

**NIST 800-88 B1:** are the data delete definition guidelines to be referenced against the legal requirements for retention schedules.
Global Education Privacy Standard (GEPS)

School / Department of Education (Data Controller)

- Written Contract
  - Clause 1
  - Clause 2

- Contract Obligations Pool
  - Obligation 1
  - Obligation 2

Control Benchmark Sets
- SDPC Set
- Set 2

NIST/ISO/IEEE "Other" standards
- You pick the technical security standard

Privacy Obligation Document (POD)
- Obligation 1 XML
- Obligation 2 XML

A machine-readable document for detailed obligations

Vendor (Data Processor)

The legalese from the DPA

The technical obligation from the legalese

Technical
Unity Enabling Privacy Expectations

Automate Contract Clause Expectations Exchange and Vendor Verification

The “POD”
(Privacy Obligation Document)

Enabled in global SIF Infrastructure
Privacy Support  
Built in privacy support, based on GDPR and Student Data Privacy Consortium (SDPC) needs.

SIF 3 infrastructure  
The REST infrastructure that starts simply and scales easily. Includes JSON conversion and is designed for the cloud. Performance is 'real' (ask Massachusetts!)

Built on SIF 2.x Specification  
Leverage existing knowledge and software. Robust, familiar data model.

xPress Roster  
Modular API design, most robust roster standard in marketplace. Compliments the Unity Data Model… you can start with xPress Roster and scale up!

Individual Education Plans (IEPs)  
1st standardized API for IEPs  
Detailed/extensive objects  
Ready for 'in District' use and Student transfers

xPress Roster  
Modular API design, most robust roster standard in marketplace. Compliments the Unity Data Model… you can start with xPress Roster and scale up!

Privacy Support  
Built in privacy support, based on GDPR and Student Data Privacy Consortium (SDPC) needs.

SIF 3 infrastructure  
The REST infrastructure that starts simply and scales easily. Includes JSON conversion and is designed for the cloud. Performance is 'real' (ask Massachusetts!)

Built on SIF 2.x Specification  
Leverage existing knowledge and software. Robust, familiar data model.

xPress Roster  
Modular API design, most robust roster standard in marketplace. Compliments the Unity Data Model… you can start with xPress Roster and scale up!

Individual Education Plans (IEPs)  
1st standardized API for IEPs  
Detailed/extensive objects  
Ready for 'in District' use and Student transfers

xPress Roster  
Modular API design, most robust roster standard in marketplace. Compliments the Unity Data Model… you can start with xPress Roster and scale up!

Individual Education Plans (IEPs)  
1st standardized API for IEPs  
Detailed/extensive objects  
Ready for 'in District' use and Student transfers

Supporting Documentation  
EDFacts Mapping, xPress Roster Mapping & Unity Adoption Guidebook - designed to help from concept to integration plan and API design all the way to development.
Example: Application Rostering

Unity Specification and Privacy Requirements – Limiting Risk

- Pre-Provision Accounts
- Scope based on Course Enrollment*

*See the Unity Adoption Guidebook pages 26 – 29

- Automatically filter sensitive data
- Automatically set retention rules
- Know who to contact with any problems

*xPress Roster example: https://xpressapi.org/user-examples/xpress-roster/*
Common Uses for Unity...

- **Library**: Access and Fines
- **Lunch System**: Access and Account Status
- **Transportation**: The perfect address for every situation
- **Reporting**: Federal and often by State
- **Attendance**: By period or as a summary
- **Assessments**: Administration, recording and between app movement
How are your vendors implementing the privacy requirements in the real world?

The Technical Blueprint.
Global Education Privacy Standard (GEPS)

School / Department of Education (Data Controller)

Written Contract
Clause 1
Clause 2

Contract Obligations Pool

Legal / Policy

Control Benchmark Sets

NIST/ISO/IEEE
“Other” standards

You pick the technical security standard

SDPC Set
Set 2

Privacy Obligation Document (POD)
Obligation 1 XML
Obligation 2 XML

A machine-readable document for detailed obligations

Technical

Vendor (Data Processor)
"Learner Centric" MA Data Hub Service

ANY Standard

“PODS”
MA Data Hub

- Manage and filter *what* data and *which* students are sent to each vendor
- Transform and anonymize data
  - Connect noncompliant vendors
  - Go beyond “cookie cutter” rostering
- Integrated, one-stop management of data integration and privacy

www.cedarlabs.com
Software Systems Enrolled:

= Data Hub Connection  = DPA on file with SDPC

Brain Bits

Software System Access

What Data?

<table>
<thead>
<tr>
<th>SCHOOL &amp; DISTRICT</th>
<th>Local Id (School)</th>
</tr>
</thead>
<tbody>
<tr>
<td>STUDENT INFORMATION</td>
<td>English Proficiency Code, First Name, Gender, Gifted Talented, Grade (Student School Enrollment1), Last Name, Local Id (Student Personal)</td>
</tr>
<tr>
<td></td>
<td>School Name (Student School Enrollment1)</td>
</tr>
<tr>
<td></td>
<td>School State Province Id (Student School Enrollment1)</td>
</tr>
<tr>
<td>CLASS ROSTER INFORMATION</td>
<td>Course Code, Course Section Code, Course Title</td>
</tr>
<tr>
<td>STAFF INFORMATION</td>
<td>First Name, Job Function Code (Staff Assignment1), Last Name, Local Id (Staff Personal)</td>
</tr>
<tr>
<td></td>
<td>School Name (Staff Assignment1)</td>
</tr>
</tbody>
</table>

Privacy and Security Obligations

Privacy Obligations

- All Privacy Obligations

Data Security Requirements

- Assess security controls
- Audit logs
- Limit failed logins
- Password complexity
- Protect system media
- Sanitize equipment
- Sanitize system media
WEBINAR:
FEBRUARY 24, 2021

Connecting and Securing in the Real World: The MA Data Hub Solution

This pilot project was designed to leverage the MA Department of Elementary and Secondary Education’s (DESE) state data collection & Cedar Labs’ “hub and spoke” architecture to branch a state reporting data connection and create an easy-to-manage data integration platform for school districts. MA DESE, and Cambridge Public Schools are leveraging the existing state data connection to branch the flow of data not just for state reporting, but to also provide additional value add services such as standards agnostic rostering and privacy enforcement.

**use promo code Unity-Feb2021 during checkout to get ‘free’ registration**
Connecting and Securing Effective Learning Ecosystems™

CIOs MUST Address

- Application Vetting
- Contracting Process
- App Management
- Integration
- Secure Data Exchange
- Quality Control
- Professional Learning
“Connecting and Securing Effective Learning Ecosystems™”

Are You Looking for Support In:

✓ **Application Vetting:** SDPC Resource Registry Workflow Tool

✓ **Contracting Process:** [National Data Privacy Agreement](#) (NDPA) *as part of Terms of Service*

✓ **App Agreement Management:** SDPC Resource Registry

✓ **Integration:** [Getting Started with Unity, Ecosystem Empowerment Guide](#)  
 *(Guide includes Implementation Planning Questions, RFP/RFI Language, Integrator Questions, Vendor Readiness Scoresheet)*

✓ **Secure Data Exchange:** Ecosystem Empowerment Guide, [Unity Adoption Guidebook](#)

✓ **Quality Control:** [Certification Registry](#)

✓ **Leverage the Community’s Work:** [Unity RFP](#) language and the NDPA
Increased interoperability without the inclusion of privacy requirements = increased RISK. Both data sharing and privacy parameters must be identified and communicated!
**Takeaways.....and Call to Action!**

**Knowing:** Increased interoperability without the inclusion of privacy requirements = increased RISK.

**Knowing:** Both data sharing and privacy parameters must be identified and communicated!

**Knowing:** The A4L Unity Specification is the ONLY pK12 technical specification addressing Interoperability **AND** Privacy

**Then:** Take advantage of addressing your data management **AND** privacy needs by demanding Unity in your RFI/RFP data system maturation plans.
Q & A…