Why NDPA?
National Data Privacy Agreement

Setting Common Student Privacy Expectations Between Marketplace Providers and End Users
Your Hosts

- **Larry Fruth PhD**  
  ○ Access 4 Learning / Student Data Privacy Consortium
  
  **“Privacy Herder”**

- **Steve Smith**  
  ○ Cambridge Public Schools
  
  **“Grandpa Privacy”**

- **Mark Williams**  
  ○ F3 Law Firm, CA
  
  **“Privacy Guru”**

- **Libbi Garrett**  
  ○ CITE, CA
  
  **“Privacy Negotiator”**
“Before I write my name on the board, I’ll need to know how you’re planning to use that data.”
Agenda

● **The Why:** Evolution of the NDPA from State NDPAs

● **The How and What:** NDPA Process Development
  ○ “Easy” issues
  ○ “Complex” issues
  ○ Draft 1 Final
  ○ Usage Issues

● **The When:** Processes for Draft 2

● Q and A
# The Why: Student Privacy Laws

<table>
<thead>
<tr>
<th><strong>CIPA</strong></th>
<th><strong>PPRA</strong></th>
<th><strong>COPPA</strong></th>
<th><strong>HIPAA</strong></th>
<th><strong>FERPA</strong></th>
<th><strong>STATE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Children’s Internet Privacy Act</strong></td>
<td><strong>Protection of Pupils Rights Amendment</strong></td>
<td><strong>Children’s Online Privacy &amp; Protection Act</strong></td>
<td><strong>Health Insurance Portability &amp; Accountability Act</strong></td>
<td><strong>Family Educational Rights &amp; Privacy Act (1974)</strong></td>
<td><strong>Legislation as well as Local Statutes and Regulations</strong></td>
</tr>
<tr>
<td>Internet filters for K–12 schools and libraries to protect children from harmful online content as a condition for federal funding.</td>
<td>Requires parental consent for any surveys that contain political, sexual, mental state, relationships, religious information</td>
<td>Requires operators of websites or online services for children under 13 that they are collecting personal information</td>
<td>Usually HIPAA does not apply because information by definition is part of “education records” under FERPA and, therefore, is not subject to the HIPAA</td>
<td>Schools must have written permission to release any information but allows schools to disclose under certain conditions</td>
<td>40 states have passed 125 student privacy laws since 2013</td>
</tr>
</tbody>
</table>

- **CIPA**
  - Children’s Internet Privacy Act
  - Internet filters for K–12 schools and libraries to protect children from harmful online content as a condition for federal funding.

- **PPRA**
  - Protection of Pupils Rights Amendment
  - Requires parental consent for any surveys that contain political, sexual, mental state, relationships, religious information.

- **COPPA**
  - Children’s Online Privacy & Protection Act
  - Requires operators of websites or online services for children under 13 that they are collecting personal information.

- **HIPAA**
  - Health Insurance Portability & Accountability Act
  - Usually HIPAA does not apply because information by definition is part of “education records” under FERPA and, therefore, is not subject to the HIPAA.

- **FERPA**
  - Schools must have written permission to release any information but allows schools to disclose under certain conditions.

- **STATE**
  - Legislation as well as Local Statutes and Regulations
  - 40 states have passed 125 student privacy laws since 2013.

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31).
FERPA Exceptions

1. Other schools to which a student is transferring;
2. Specified officials for audit or evaluation purposes;
3. Appropriate parties in connection with financial aid to a student;
4. Organizations conducting certain studies for or on behalf of the school;
5. Accrediting organizations;
6. To comply with a judicial order or lawfully issued subpoena;
7. State and local authorities, within a juvenile justice system, pursuant to specific State law;
8. Appropriate officials in cases of health and safety emergencies;
9. School officials with legitimate educational interest;
## Student Privacy Laws

**FERPA**

School officials with legitimate educational interest:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performs an <strong>institutional service</strong> or function for which the school or district would otherwise use its own employees;</td>
<td><strong>Is under the direct control of the school</strong> or district with regard to the use and maintenance of education records; and</td>
</tr>
<tr>
<td>Has been determined to meet the criteria set forth in the school’s or district’s annual notification of FERPA rights for being a school official with a <strong>legitimate educational interest</strong> in the education records;</td>
<td><strong>Uses education records only for authorized purposes</strong> and may not re-disclose PII from education records to other parties (unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA).</td>
</tr>
</tbody>
</table>
Student Privacy Laws

FERPA

School officials with legitimate educational interest. Data Privacy Agreements (DPA) should cover:

- Security and Data Stewardship Provisions.
- Collection Provisions.
- Data Use, Retention, Disclosure, and Destruction Provisions.
- Data Access Provisions.
- Modification, Duration, and Termination Provisions.
The National Data Privacy Agreement

Now that schools know they SHOULD have a Data Privacy Agreement (DPA) What’s Next?

Fun Facts:
• 13,000+ US Public School Districts
• 85% of Them Have Less Than 5,000 students – Many CIO’s Teach Daily!
• The Average US School Has Anywhere Between 400 and 1,000 Applications
• “Freeware” or ”Freemium” Products Are Exploding
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

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://privacy.A4L.org
- https://sdpc.A4L.org
No One Gets It!

Everyone Gets It!

No One Gets It!
SDPC Origin

The SDPC:

- Built upon work done in CPS
- 12+ years working with vendors
- Developed in house tools
- Awareness building
- Standardized DPAs
- Expanded across MA
SDPC Goals

1. Establish a community of stakeholders who have various needs addressed through policy, technology and/or effective practice sharing around effective privacy management.

2. Development of tools and resources to address operational issues not currently being addressed.

3. Development of a clearinghouse of student data privacy operational issues and resources to support schools, districts, states and vendors in managing those issues – no matter where the resources originate.

4. Identify projects that have on-the-ground and real-world impact on student data privacy enabling schools, districts, state and vendors find resources, adapt them to their unique context and implement needed protections.

5. Leverage partnership organizations working in the privacy space to have their good work utilized and no reinvention of existing work.
Privacy – By The Numbers...
the Student Data Privacy Consortium (SDPC)

A Community Maturing!

✔ After Three Years, 13 States Using Similar DPAs
✔ Legal Project Team Established Working for a Year
✔ Establish a “Common Denominator” for Easy of Use and For Clarity Around State Requirements
✔ Two Community Review Periods Resulting in Over 200 Comments and Suggestions (65% Accepted)

25 State-wide Alliances

Tools for:
Privacy Contract Building
Application Inventory & Searchable Database
Application Contract Management
Global Education Privacy Standard (GEPS)

Tactical Privacy Information
contract to implementation

34 million
Students supported by Tools

9731
School Districts represented

4
Countries Collaborating on Privacy Issues

45990
Signed Vendor Agreements

6959
Applications in Database

43828
Signed “Piggyback” Exhibit E
Too Many Contracts … and Not Much Time!

Wouldn’t it Be Great If You Could:

- Save Resources (time, money, etc.) With ONE Data Privacy Agreement in ALL of Your Agreements with Vendors
- “Piggyback” Off Other Signed Agreements By Districts in Your Alliance?
- Seamlessly and Transparently Communicate Those Agreements to Staff, Parents, Etc.
What are Alliances doing to help?

Lots of resources to assist with process

Training Sessions

Vendor Support

www.StudentDataPrivacy.net
Legal Work : Feb 2019 to Present

2019 A4L/SDPC Meeting:
- Kick off if Legal Working Group
- Goals of NDPA Summer 2019

18 Months of meetings:
- Districts, Alliances, SEAs & Vendors
- Clause by clause discussions
- Suggestions gathered
- Security sub-group
- Hit a wall Feb 2020 - then COVID
- Completed via Alliance working group

April 2020:
- Alliance working group formed
- Completed NDPA Draft 1 June 2020

Two Rounds of Community Comments:
- Approximately 200 Comments
- Roughly 60% Accepted
- Many duplicates

NDPA V1 Released July 2020:
Introducing…
The National Data Privacy Agreement V1

✔ Goals:
  • Further increase consistency across Alliance DPAs
  • Standardize the DPA Format so it looks the same across Alliances
  • Ease logistics of implementing
  • Identify common legal requirements across jurisdictions
  • Provide mechanism to add other jurisdiction specific requirements
  • Standardize terminology & definitions across jurisdictions and working groups (Legislative)
  • Greater impact on, and buy in from, the vendor marketplace = Adoption
# Making Agreements “Simple”

<table>
<thead>
<tr>
<th>NDPA Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section</td>
<td>Cover Page</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>

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. Special Provisions. Check if Required

   - If checked, the Supplemental State Terms and attached hereto as Exhibit “G” are hereby incorporated by reference into this DPA in their entirety.
   - If checked, LEA and Provider agree to the additional terms or modifications set forth in Exhibit “H”. (Optional)
   - If checked, the Provider, has signed Exhibit “E” to the Standard Clauses, otherwise known as General Offer of Privacy Terms
Conversation Points - “The Issues”

- “Easy” Issues
- “Complex” Issues
- Draft 1 Final
- Usage Issues
Q and A

○ When Will Version 2 Be Developed?
○ How does Exhibit E work?
○ Does each state have to have their own DPA?
The Result – Common Expectations!

End Users

Here is the data we will give you and details on how we want it treated

Automated

Here is how we have treated the data and details on how we can prove it to you

Providers

Increased interoperability without the inclusion of privacy requirements = increased RISK. Both data sharing and privacy parameters must be identified and communicated.
Steve Smith
ssmith@cpsd.us

Mark Williams
mwilliams@f3law.com

Libbi Garrett
libbi.garrett@cite.org

Larry Fruth II, PhD
lfruth@A4L.org

Find Out More
https://www.privacy.a4l.org