Data Breaches & Interoperability

What Privacy Leaders Need to Know

Alex Jackl

Welcome & Introductions

Overview

- **Surging Data Breaches:** K–12 schools are facing a spike in cyberattacks, that potentially expose personal information of millions of students and teachers . Districts now hold vast **troves of sensitive data** and thus have become prime targets for hackers .
- **Third-Party & Interconnected Systems Risk:** Modern schools depend on **numerous connected apps and third-party services**, which greatly expands the attack surface. A vulnerability in one vendor's system can cascade into widespread consequences. The is a **need for vendor oversight and security requirements** to protect shared data .
- **Why Now:** Data volumes and digital integrations in K–12 have never been higher, just as cyber threats are intensifying. In recent years schools have dramatically increased their use of online programs and cloud services. **School data leaders must act now** to prevent breaches from disrupting learning and eroding public trust.

Agenda

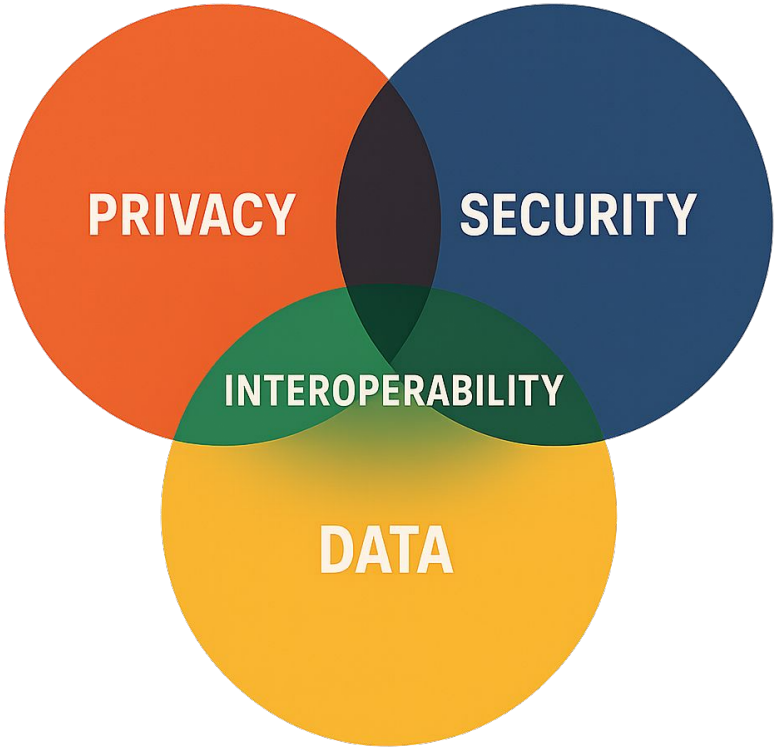
- How Poor Interoperability Contributes to Breach Risk
- What Privacy Leaders Should Ask & Demand
- Frameworks & Standards That Help
- Deep Dive: The Danger of “Sucking Everything Out” via API
- Case Study: PowerSchool Breach
- Aligning Interoperability & Legal Requirements
- Other Considerations & Emerging Issues
- Summary + Key Takeaways
- Actionable Steps
- Q&A

Definitions

Interoperability: Student, teacher, and system data can securely move across platforms (student information systems, assessment tools, learning management systems, etc.) without duplication, confusion, or loss of meaning—while supporting compliance, privacy, and efficiency.

Data Breach: Student or staff records are exposed through insecure vendor systems, poorly managed file exchanges, or insufficient oversight of who can access what data. Unlike a simple "incident" (which might just be a technical hiccup), a data breach specifically involves loss of control over private information.

It all comes together.



Poor Interoperability to Breach Risk

Common Interoperability Design Issues:

- Overbroad data access (too much data given to vendor / system)
- Weak or missing segmentation / least-privilege / role-based access controls
- Insecure APIs / endpoints, lack of encryption, lack of monitoring
- Poor vendor/subprocessor oversight

What You Should Ask & Demand

- Data Flow Mapping & Inventory
  - What data, from what system, to whom, via what mechanism (API, file share, push/pull)
  - Ownership, responsibilities, who is controller / processor (or equivalent)
- Access Control & Least Privilege
  - Role-based access, checking that vendors/subprocessors only get what they need
- Contractual & Technical Safeguards
  - Encryption (in transit / at rest)
  - Authentication (MFA, strong credential policies)
  - Logging & monitoring, anomaly detection
  - Data minimization (collect/store only needed data)

What You Should Ask & Demand

- Vendor Management & Oversight
  - Vendor contracts (DPAs), audit rights, security assessment, certifications
  - Subprocessors list, ability to vet or require compliance
- Incident Response & Notification Processes
  - Vendor obligations in breach / exfiltration scenarios
  - Timeliness, transparency

Frameworks & Standards That Help

- **SIF / SIF Unity (Systems Interoperability Framework / Unity Specification)**
  - What SIF Unity provides: built-in security, transport, data model, and privacy controls.
  - Strength: designed for operational data exchange across PK-12, with alignment to privacy governance.
- **NDPA (National Data Privacy Agreement) / SDPC Model Agreements**
  - Purpose: consistent contractual terms across states, lowering vendor and district overhead.
  - Key: clarifies vendor obligations, breach response, and security practices.

Frameworks & Standards That Help

- **Other Standards Ecosystem**
  - **GESS (Global Education Security Standard):** Crosswalks major security controls to a K-12 context
  - **CEDS (Common Education Data Standards):** Provides shared vocabulary and definitions that can be mapped into operational standards, reducing ambiguity and misinterpretation.
  - **PESC (Postsecondary Electronic Standards Council):** Bridges into higher education and workforce, ensuring privacy and data portability beyond K-12.
  - **HR Open Standards:** Focuses on HR, employment, and workforce interoperability — critical when student data eventually transitions to workforce data.
- **Legal / Regulatory Alignment**
  - **FERPA**: educational record protections, school official exception, “legitimate educational interest.”
  - **State privacy laws:** new obligations around breach notifications, consent, and vendor contracts.

Deep Dive: The Danger of an API

- What that Looks Like in Practice
  - API endpoints returning more data than needed (“over-fetching”)
  - Shared or open endpoints that aggregate data across schools or systems without filtering

Deep Dive: The Danger of an API

- Consequences
  - More attack surface / more sensitive PII exposed
  - Increased risk if credentials compromised
  - Regulatory / legal risk (violations, penalties)
- Mitigation Strategies
  - Use of filtered views, scopes, limited fields in APIs
  - Tokenization / data masking / pseudonymization where possible
  - Strong authorization checks per request

Case Study: PowerSchool Breach

1. What Happened
    - Timeline: December 2024 discovery; method: stolen credential; which system: internal support portal; data involved (names, SSNs, medical info, grades, etc.)
2. What Interoperability / Access / Vendor Management Issues It Illustrates
    - Vendor/subprocessor credentials being a weak link
    - Insufficient segmentation of systems (e.g. internal support tool having access to broad datasets)
    - Gaps in authentication / multi-factor / least privilege
3. Regulatory / Legal / Settlement Impacts
    - State lawsuits (e.g. Texas AG suit) over deceptive trade practices, misleading statements about security practices.
    - Requirement / pressure to offer credit monitoring, identity protection, notifications etc.

Interoperability & Legal Requirements

- FERPA and State Law Alignment
  - Understand what legal definitions (education records, school official, legitimate educational interest) demand about access and use
  - State laws may impose additional restrictions (on health data, special education, disability, etc.)
- Contractual Tools (DPAs, NDPA, Vendor Agreements)
  - Using NDPA / standard agreements to ensure consistent terms
  - Ensuring modifications comply with local legal requirements

Interoperability & Legal Requirements

- Technical Standards + Certification
  - Adopting standards like SIF Unity to ensure privacy built in, not bolted on
  - Certifications, audits, compliance verification
- Governance and Oversight
  - Internal privacy program: roles, responsibilities, oversight (privacy officers, data protection officers)
  - Regular reviews of vendor access, system architecture

Other Considerations & Emerging Issues

1. Cross-jurisdictional data flows (states, possibly international) & how laws differ
2. Emerging threats: AI tools, third-party data brokers, analytics vendors
3. Privacy vs. usability trade-offs (data needed for insights vs risk)
4. Transparency to stakeholders (parents, students, teachers)

Summary + Key Takeaways

1. Poor interoperability design increases breach risk in multiple ways (over-sharing, weak controls, vendor gaps).
2. Privacy leaders should ask the right questions: data flow, access, vendor practices, technical safeguards.
3. Frameworks like **SIF Unity**, contractual tools like the **NDPA**, and definitional standards such as **CEDS, PESC, and HR Open Standards** together provide a more complete foundation for safer interoperability.
4. Align interoperability with **FERPA and state law** while maintaining strong vendor oversight and governance.

Q&A

Actionable Steps

- Conduct an audit of all data flows across systems & vendors
- Review existing vendor contracts / DPAs for clauses about minimal data, access control, breach obligations
- Evaluate whether any APIs or data endpoints are over-broad / need tightening / least-privilege
- Consider adopting SIF Unity or related standards where possible
- Use the NDPA or state-adapted DPAs to standardize vendor expectations

Thank You

- https://a4l.org/
- Email Penny Murray to add someone to the mailing list for this webinar series: pmurray@a4l.org
- Thank you!