IO education

IMPROVING EDUCATIONAL OUTCOMES

Presentation by

Doug Mesecar, Vice President, Strategic Partnerships, IO Education

Before the

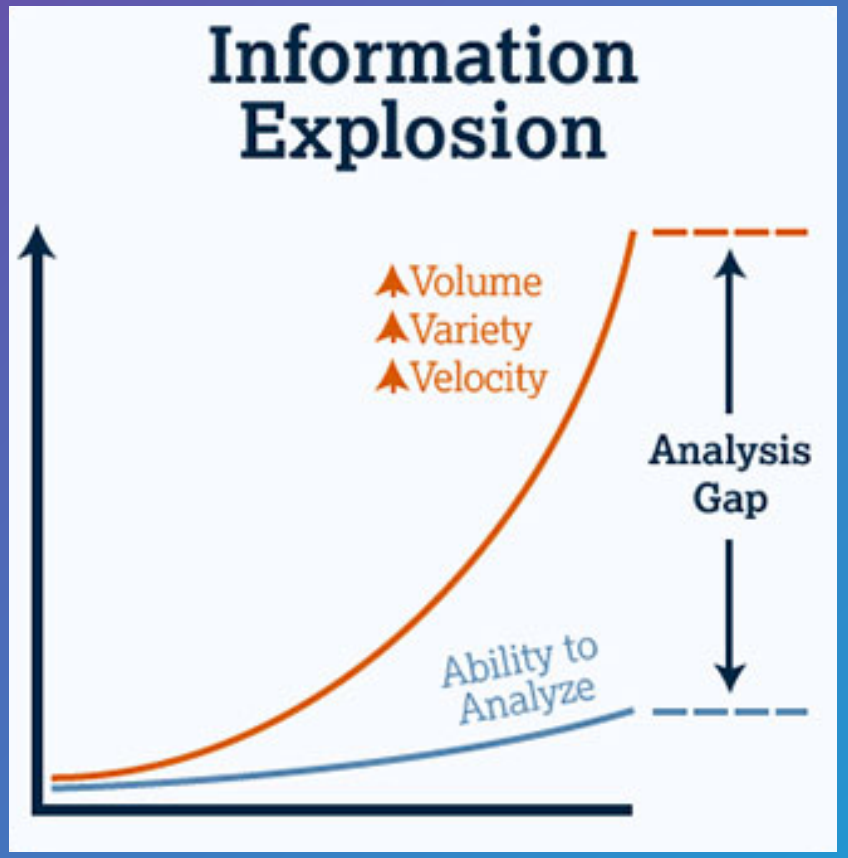
Legislative Council Study Committee on School Data

Wisconsin State Legislature

September 14, 2016

The Power of — and Responsibility for — Using Student Data to Improve Educational Outcomes

“Data is not about adding more to your plate; data is about making sure you have the right things on your plate.”
—Unknown



Agenda

- About IO Education
- IO's Privacy Policies
- Student data across the country
  - California
  - Colorado
  - Other states
- ESSA
- Best practices around student data privacy

Our mission is to empower educators through data to improve educational outcomes

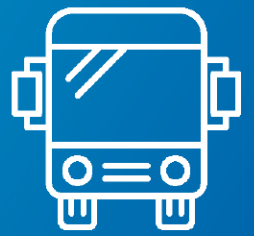
We are a K-12 technology platform that delivers the **right data** to the **right people** at the **right time**

COMPANY APPROACH

IO Education exists to:

Drive student achievement

Increase educator effectiveness



Deliver operational efficiency

We do this by:

» Consolidating all data: Aggregating all of your data trapped in local and districts data sources and consolidating it to the K12 data platform

» Creating robust insights: Create the right view of the aggregated data for the right people at the right time, allowing them to analyze, monitor and share their insight

» Developing & tracking personalized plans of action: Leveraging the new insights allow educators to develop and implement personalized success plans that are monitored and adjusted on a regular basis

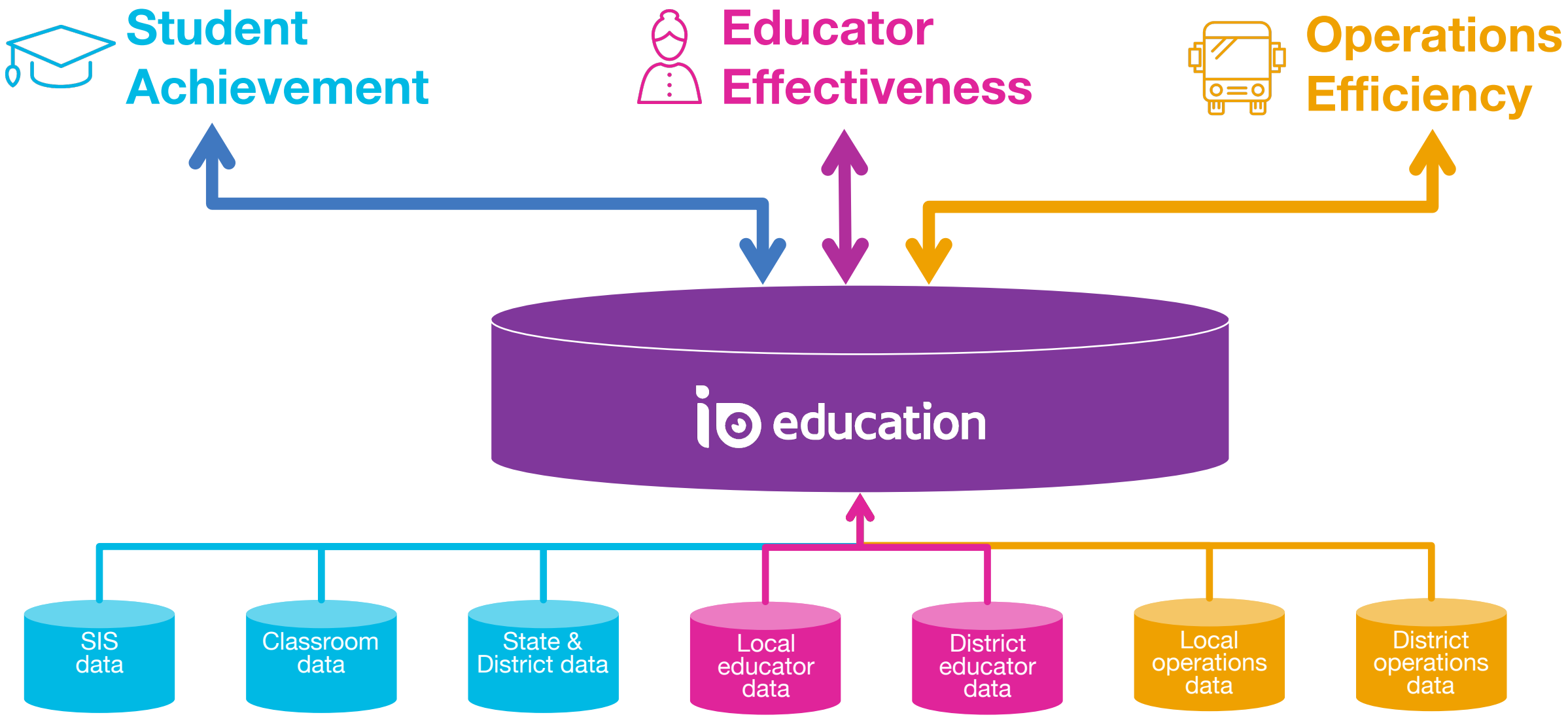
info@ioeducation.com

5,136
SCHOOLS

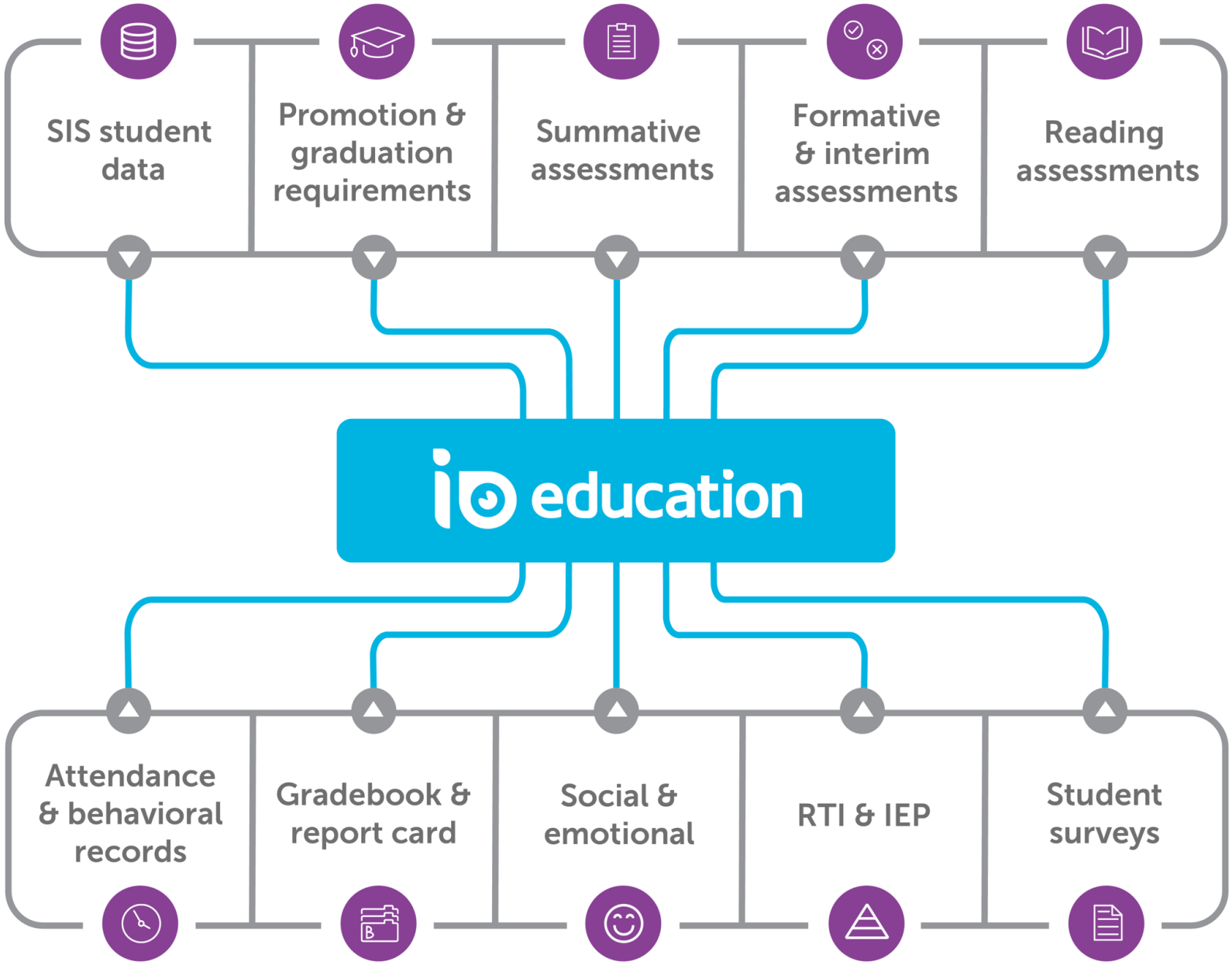
102,076
EDUCATOR USERS

4,784,230
STUDENT RECORDS

We break down data silos



Data in the Classroom



IO's Student Data Privacy Practices

- With over 18 years of experience, IO provides a secure and private platform that enables school districts to integrate data from their various sources and securely store that data in one place.
- School districts decide which data is provided and stored in our platform. Once data is provided to us, we take care of it as if it were our own children's information.
- IO has a "Pledge to Parents" on its website at https://ioeducation.com/pledge-to-parents/ that covers important privacy policies in simple to understand language.

IO's Student Data Privacy Practices

- IO Education ensures it meets or exceeds applicable requirements in federal and state laws, regulations, district policies, as well as private industry best practices.
- Third parties and contractors working with IO are subject to IO's policies, requirements and security protocols.
- IO has a designated Privacy Officer who ensures polices, practices and procedures are followed with fidelity.
- IO's Privacy Policy is posted on our website at https://ioeducation.com/privacy-policy/
- IO has signed the Student Privacy Pledge: https://studentprivacypledge.org

IO Complies with Student Data Laws

- IO stores, manages and provides data visualizations in compliance with FERPA.
- IO relies on the district's compliance with FERPA's provisions regarding the release of PII either through district obtaining parental consent to share PII with IO and/or the district is using the "School Official" exemption under FERPA to release data to IO.
- COPPA does not apply to IO's platform largely because the student is not the end user.

IO's Student Data Privacy Practices

We Do Not:

- Collect, maintain, use or share student personal information beyond that needed for authorized educational or school purposes as contractually agreed to with the educational institution;
- Sell student personal information to anyone for any reason;
- Share any personally identifying information unless directed to by the school district or by the parent/student, except in response to subpoenas, court orders or legal process, to the extent required or as restricted by law;
- Use or disclose student information for the targeting of advertisements to students;
- Build a personal profile of a student other than what is required and authorized by the school, school district or the state department of education;
- Retain student personal information beyond the time period necessary for the authorized educational purpose(s) or as authorized by parent (or student of age).

IO's Student Data Privacy Practices

We Do:

- Collect, use, share, and retain student personal information only for purposes for which we were authorized by the educational institution or the parent/student;
- Support access to and correction of student personally identifiable information by the student or their authorized parent through the educational institution;
- Maintain comprehensive security and privacy policies that are designed to protect the security, privacy, confidentiality, and integrity of student personal information against risks such as the unauthorized access or use, or unintended or inappropriate disclosure through the use of appropriate administrative, technological, and physical safeguards;
- Require that our vendors with whom student personal information may be shared in order to deliver the educational service when authorized by the educational institution are subject to IO's policies for the given student personal information.

Across the Country

- Colorado
- California
- Other states

Colorado

- Student Data Transparency and Security Act
- Bipartisan effort that passed unanimously though state legislature, signed into law in June 2016
- Timeline:
  - After August 10, 2016 – CDE and districts cannot enter into or renew a contract with entities that refuse to accept terms of updated contracts and provisions of the bill.
  - March 1, 2017 – CDE must create and make available a sample student information privacy and protection policy for districts
  - December 31, 2017 – Districts to adopt a student information privacy and protection policy
  - July 1, 2018 – Small rural districts to adopt a student information privacy and protection policy

Colorado cont’d

- Like California, the new law applies to both educational institutions and vendors. Defines student personally identifiable information (SPII)
- Defines "School Service Contract Provider" and "School Service On-Demand Provider"
- As of August 10th 2016, vendors contracting with districts must contractually agree to comply with certain requirements if they are to collect information about students.
- Every district must list the school services they use on their website, including a copy of each contract, along with other important and relevant district policies and practices.

Colorado cont’d

- Some of the bill’s requirements for vendors:
  - Vendors can only collect data for the purposes specified in the contract. If they would like to use data in another way, they must receive consent from the parent or student (if over 18). The bill also bans selling information or using it for targeted advertising. Data cannot be used for any purposes beyond those outlined in the contract. If a vendor would like to do so, they must obtain parental consent.
  - Vendors must also notify the educational institution with which they are contracting if a data breach is discovered or if the privacy policy undergoes any changes.
  - Vendors may share data with subcontractors only if the subcontractor contractually agrees to comply with these rules and restrictions.
  - Vendors must also maintain a comprehensive information security program, ensuring that student data is accessed and used appropriately.
  - Vendors must destroy information upon request by the education institution, or at the end of the contract or its specified timeline.
  - In addition to potential liabilities, material breaches of these requirements may result in the education entity terminating use of the service.

California

- SOPIPA - first legislation to apply to vendors specifically
  - In effect January 1, 2016

- AB1584 - works with SOPIPA requires contracts between local educational agencies and third parties to include specified provisions about the security, use, ownership, and control of pupil records.

Other states

- NYC (and New York State)
- Generally
  - Lack of consistency
  - Shifting focus
  - Politics
  - District/school practices
    - Not always consistent in knowledge / implementation
    - Need training

The ESSA Impact on Data: Accountability

District	Indicator Data Points	Grades	# Schools	Total Indicator Data Points
ES	16	3	10	480
MS	16	3	4	192
HS	16	1	2	32
Total				**704**

Schools with 5 subgroups & 4 indicators

The ESSA Impact on Data: Reporting

Assessment & Accountability

District	Reporting Data Pts	Grades	Total	# Schools	Grand Total
ES	78	3	234	10	2,340
MS	78	3	234	4	936
HS	67	1	67	2	134
Total					**3,410**

Reporting Data Points In District

Best practices around student data privacy

- Business model
- Privacy Officer - somebody has to own it; constant vigilance
- Clearly articulated and publicly available (website) privacy policy for website and/or platform
- Insurance
- USDE Model Terms of Service - http://ptac.ed.gov/sites/default/files/TOS_Guidance_Jan%202015_0.pdf
- FERPA
- Both sides of the equation are important: District and vendor partnership to protect student data
- Resources: PTAC, FerpaSherpa, iKeepSafe, commonsense education, CoSN, Education Technology Industry Network (SIIA)

IMPROVING EDUCATIONAL OUTCOMES

Questions?

dmesecar@ioeducation.com

703.887.3738