Safeguarding DATA

DQC DATA QUALITY CAMPAIGN — Using Data to Improve Student Achievement

Getting the Facts Straight

about Education Data

Education data can empower educators, students, parents, and policymakers with the information they need to make the best decisions to improve student achievement, information that can move the nation toward an education system in which every student graduates prepared for college and career. Safeguarding the privacy of student data is a critical component of effective data use, and this data stewardship is a shared responsibility. Recently, conversations about how education data are collected and used, and the ways in which student privacy is safeguarded, have been taking place around the country. An important part of these conversations is ensuring that existing privacy laws and practices are well understood and that misconceptions about data use and privacy are addressed. This document dispels the most common myths with concise talking points and related resources. Information about the number of states reporting an activity is based on Data Quality Campaign's (DQC) *Data for Action 2013.*

MYTH: The US Department of Education collects academic and other information about individual K–12 students.

FACTS:

- The Higher Education Opportunity Act (HEOA) of 2008, No Child Left Behind (NCLB) legislation amending the Elementary and Secondary Education Act (ESEA), the Education Sciences Reform Act (ESRA) of 2002, and the Individuals with Disabilities Education Act (IDEA) **prohibit the creation of a federal database** with students' personally identifiable information (i.e., information such as Social Security Number).
    - Section 113 of HEOA: "Except as described in subsection (b) [relating to systems necessary for operations of specified Higher Education Act programs and previously in use by the Department], nothing in this Act shall be construed to authorize the development, implementation, or maintenance of a Federal database of personally identifiable information on individuals receiving assistance under this Act, attending institutions receiving assistance under this Act, or otherwise involved in any studies or other collections of data under this Act, including a student unit record system, an education bar code system, or any other system that tracks individual students over time."
    - Section 9531 of ESEA and NCLB: "Nothing in this Act (other than section 1308(b) [relating to a migrant record system] shall be construed to authorize the development of a nationwide database of personally identifiable information on individuals involved in studies or other collections of data under this Act."
    - Section 182 of ESRA: "NATIONAL DATABASE- Nothing in this title may be construed to authorize the establishment of a nationwide database of individually identifiable information on individuals involved in studies or other collections of data under this title."
    - Section 616 of IDEA: "(ii) Rule of construction.-- Nothing in this title shall be construed to authorize the development of a nationwide database of personally identifiable information on individuals involved in studies or other collections of data under this part."
- The federal government is authorized to publicly report specific *aggregate-level data only*.
- Federal law prohibits the reporting of aggregate data that could allow individuals to be identified.
- The federal government **does not** have access to the student-level information housed in state data systems. (Watch this video for more on the entities that use student data.)

- The Common Core State Standards **are not** a mechanism for federal data collection. There is no new federal data collection associated with the assessment consortia, and states using the consortia, assessment tools do not have any different reporting requirements than non-participating states.
- **No** student-level data from the Partnership for Assessment of Readiness for College and Careers and Smarter Balanced Assessment Consortium assessments are shared with, or collected by, the federal government.
- Common Core (and related assessment consortia) **does not** authorize the sharing of student data between states.

MYTH: The federal government is using grants such as The Statewide Longitudinal Data Systems (SLDS) grant program, The American Recovery and Reinvestment Act (ARRA), and Race to the Top as a way to drive a national/federal collection of student information into a single database.

FACTS:

- States that receive grants from the federal government **are forbidden** to report any student-level data to the federal government in return *(see HEOA, NCLB, SLDS, and IDEA language above describing this prohibition)*.
- States were building data systems and collecting the necessary information to improve education within each state years before the federal government introduced grants to support this work.
- As a condition of receiving any ARRA funding, states committed to building their SLDS with elements described in the America COMPETES Act (ACA); the 12 elements in the ACA align with DQC's 10 Essential Elements.
- The State Fiscal Stabilization Fund (SFSF) under ARRA **did not** encourage or require the use of SFSF funds for the development of these data systems. However, operationalizing the 12 ACA elements was a requirement of receiving funding.
- States have been building student-level data systems for more than a decade to inform policy and practice; the average state reported meeting five of the DQC's 10 Essential Elements prior to the first federal grant awards to states for this purpose. The systems provide educators with the information (e.g., cohort graduation rates, growth measures, early warning systems) needed to inform their practice.
- States are committed to building and supporting their own data systems; as of 2013, 41 states are providing state funding for their P–20W SLDS.

MYTH: The National Education Data Model (NEDM) is a federally driven collection of hundreds of pieces of sensitive individual student information.

FACTS:

- The NEDM **is not** a data collection and **does not** contain any data; no state or district is submitting data to the federal government based on this model.
- The NEDM is a technical resource that was developed at the national level; its use **is not** required as a condition of any funding or collection.
- The NEDM is a framework describing the types of data that individual districts and states *may choose to use* to answer their own questions about policy and practice.
- The NEDM was funded by the National Center for Education Statistics (NCES), managed by the NCES Forum (comprising state and district representatives from every state), and received technical assistance from the Council of Chief State School Officers.
- A data model is a representation that shows how unstructured data in a database could be organized or connected.

MYTH: The Common Education Data Standards (CEDS) is a mandatory initiative to collect hundreds of pieces of sensitive data about students.

FACTS:

- CEDS **is not** a data collection, nor a federal unit record system, and it **does not** collect any data.
- CEDS is a voluntary project to list consistent names for data elements that states or districts **may** wish to collect and to show how these elements could be organized in a model. A data model is a representation that shows how unstructured data in a database could be organized or connected.
- CEDS is a technical resource that was developed to help states and districts to improve the quality of and organize the data they already collect.
- No state is required to adopt the CEDS naming conventions. Those that opt to do so may choose to adopt only certain parts.
- Responding to states' desire to improve their individual data standards, NCES established a technical working group to develop the voluntary CEDS framework. This working group, now called the CEDS Stakeholder Group, includes representatives from across the P–20W field.

MYTH: The Family Educational Rights and Privacy Act (FERPA) has been weakened by recent regulations.

FACTS:

- The 2008 and 2011 regulations were direct responses to state requests for clarification of FERPA regarding the role of the state in using student data while maintaining privacy protections around personally identifiable information.
- The US Department of Education clarified FERPA's application to state longitudinal data systems through a public process in response to conversations among states, education stakeholders, and public stakeholders over several years and across two administrations.
- The 2008 and 2011 clarifications aligned FERPA with other federal laws requiring states to link data systems and use student data for evaluation and school and district accountability.
- Prior to these clarifications, states were unclear about basic, permissible activities, including whether postsecondary institutions can share data with state and local education agencies for the purpose of understanding student pathways to success (such as the data in high school feedback reports), whether state-level data could be used for research to improve instruction, and whether the state can transfer student academic records to a receiving district when a student moves.
- These changes were accompanied by provisions designed to tighten privacy protections and provide for fuller FERPA enforcement.
- When the US Department of Education issued FERPA clarifications, it also took steps to build capacity within the department to provide technical assistance to states and districts on strengthened privacy protections; these steps included hiring a chief privacy officer, establishing the Privacy Technical Assistance Center, and issuing technical briefs providing guidance and best practices on protecting personally identifiable information.

MYTH: FERPA is the only law protecting student privacy, and states are not addressing this issue.

FACTS:

- While FERPA sets limits on how personally identifiable data can be accessed and shared, states also have their own policies and practices, and many have state laws that parallel FERPA designed to ensure the privacy and confidentiality of data. Virtually all states also have laws that address data security and security breaches.
- Nearly all states education agencies (48) have established governance bodies charged with managing the collection and use of data, including determining how those data will be kept secure and confidential.
- Nearly all states (45) have established policies that determine what type of data is available to select stakeholders—like teachers and principals—who will use it to improve instruction.

- Nearly all states (45) make their data privacy policies publicly available (other states may have internal documentation).
- States are responsible for developing policies that determine *how* student data will be protected from inappropriate sharing or use.

MYTH: Efforts to centralize the collection and storage of student information are increasing the risk of inappropriate access and use of this information.

FACTS:

- Storing data in multiple fragmented district-level systems increases the chance that student data will be mismanaged or inappropriately accessed.
- Centralized systems, such as statewide longitudinal data systems, ensure that data collection, storage, and access meet a uniform set of protections that limit the risk of inappropriate access and use.
- District-level vendor contracts can be costly and can create redundancy across the state. If a state chooses a statewide vendor, it can reduce costs for districts, ensure that privacy measures are implemented consistently and effectively across the state, and relieve districts of management and security burdens.

MYTH: States are selling student-level data to vendors and corporations who will use those data to develop new products to market to students.

FACTS:

- States and districts **cannot** and **do not** sell student information, and the limited information that states and districts do collect is used for the purpose of informing policy, practice, and research to improve education and delivering educational services to students. Service providers who contract with states or districts to provide data management services also are prohibited from selling student data *(as prescribed in FERPA; see above for reference)*.
- In response to external research and transparency requests, some states charge fees to assemble data sets to cover labor and resource costs associated with responding to these data requests.
- FERPA ensures that any individual or entity that a state or district authorizes to access its data must (1) use student data only for authorized purposes; (2) protect the data from further disclosure or other uses; and (3) destroy the data when no longer needed for the authorized purpose.
- Out of necessity, states and districts have always contracted with for-profit and nonprofit partners to transform their data into actionable information.

MYTH: States are collecting and sharing an inappropriate amount of student-level data.

FACTS:

- States **do not** have access to the full array of data collected and maintained by schools and districts.
- States collect a limited amount of student-level information that is commensurate with state-level responsibilities. State data can provide a rich set of contextual information to supplement district-level data and guide local improvement efforts.
- Not all of the student data transferred to the state and used for state activities and reports is personally identifiable (i.e., information that could be used to identify individuals). Data can be de-identified (i.e., information that would allow the identification of an individual is removed) or aggregated (i.e., combined with data from many other students such that an individual's data cannot be identified).

MYTH: The most effective privacy laws and policies implement the same protections for all categories of data.

FACTS:

- Data can be used in several different ways (e.g., for districts to improve education experiences, for service providers to improve their services, or for service providers to market their products). Policymakers have a responsibility to govern these different uses, but they need to do so differently.

- Existing laws already govern different uses of data. FERPA, along with many state laws, apply to the data collected by districts and used to improve education experiences in the classroom and decisionmaking around funding, staffing, and programming. The Protection of Pupil Rights Amendment ensures that parents have the right to consent to US Department of Education-funded surveys or analyses that may ask students about sensitive topics (e.g., political affiliations, sexual behavior and attitudes, self-incriminating behavior).

- As online services are increasingly used in classrooms, other federal laws (including the Children's Online Privacy Protection Act), state laws, and contracts with online service providers must govern how these student-reported and use-generated data (including metadata) are used and safeguarded.

- When creating policies to safeguard the data collected by districts, states should ensure that their policies contain the following foundational components:

  - a statement of the purposes of the state's privacy policies, including an acknowledgment of the educational value of data and the importance of privacy and security safeguards;
  - selection of a state leader and advisory board responsible for ensuring appropriate privacy and security protections, including for developing and implementing policies and for providing guidance and sharing best practices with schools and districts;
  - establishment of a public data inventory and an understandable description of the specific data elements included in the inventory;
  - strategies for promoting transparency and public knowledge about data use, storage, retention, destruction, and protections;
  - development of statewide policies for governing personally identifiable information; and
  - establishment of a statewide data security plan to address administrative, physical, and technical safeguards.

DQC DATA QUALITY CAMPAIGN

The Data Quality Campaign (DQC) is a nonprofit, nonpartisan, national advocacy organization committed to realizing an education system in which all stakeholders—from parents to policymakers—are empowered with high quality data from early childhood, K–12, postsecondary, and workforce systems. To achieve this vision, DQC supports policymakers and other key leaders to promote effective data use to ensure students graduate from high school prepared for success in college and the workplace. For more information, visit www.dataqualitycampaign.org.