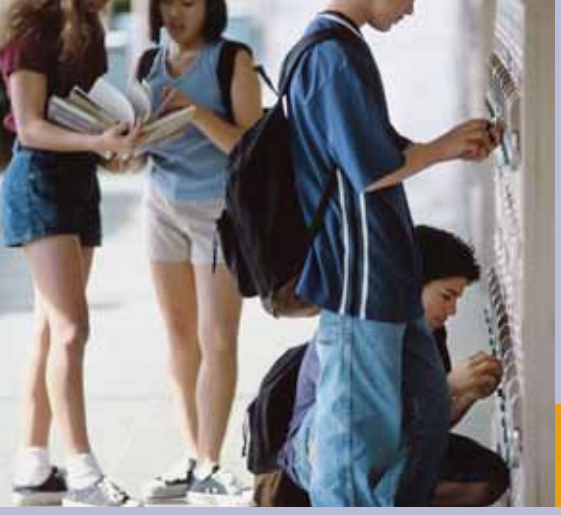

Supporting Data Use While Protecting the Privacy, Security and Confidentiality of Student Information

A Primer for State Policymakers

July 2011

There is a clear national consensus that the American education system must meet a bold new expectation — that every student will graduate from high school college and career ready — and do so with increasingly scarce resources. Policymakers and education leaders at all levels recognize that meeting this goal requires better decisionmaking, increased efficiencies and greater transparency — none of which can be accomplished without the effective use of data.

The education sector is beginning to embrace a culture that values, demands and uses data to support improved decisionmaking at every level — in classrooms, at kitchen tables and in state capitols. This shift is due in large part to state policymakers' leadership over the last six years in building statewide longitudinal data systems that collect and connect student-level data over the course of students' educational careers. States are now focused on critical actions to make sure these data can be used: linking data across disparate data systems, providing timely and appropriate access to stakeholders, and building stakeholders' capacity to use this information responsibly and effectively.

While using education data is indispensable to policy, management and instructional decisions, this work must be balanced with appropriate protections for student data. The collective efforts to maximize the great potential of data must be accompanied by the necessary actions to:

- **Meet the moral and legal responsibility to respect the privacy and the confidentiality of students' personally identifiable information;**
- **Mitigate risks related to the intentional and unintentional misuse of data,** which are amplified by the digital nature of today's society in which more information — in education and every sector — is housed and shared in electronic and web-based forms; and
- **Ensure clarity around roles and responsibilities,** including states' authority to share data, in what form the data can be shared, at what level of detail, with whom and with what protections in place.

Adequate and strategic action on these fronts does not preclude the effective use of data. The education sector is not alone in its efforts to achieve this critical balance; nearly

Privacy, Security and Confidentiality Defined

In its brief, *Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records,* the National Center for Education Statistics summarizes the following concepts, which are critical to understand as part of strategies to protect student information:

Personally identifiable information: information that can be used to distinguish or trace an individual's identity

Privacy: individual autonomy and personal control over who has access to a person's own information — when, how and why?

Security: physical protection of data

Confidentiality: obligations of those whose have access to another individual's personally identifiable information

every other sector has been transformed by the use of technology and data and has tackled the challenge of ensuring the privacy, security and confidentiality of personal information. Education can learn from their experiences.

This publication outlines **three overarching responsibilities of state policymakers** to protect the privacy, security and confidentiality of students' personally identifiable information and a **series of questions about state policies and practices for state officials** responsible for the stewardship of student data and state data systems to both protect student data and maximize their use to improve student achievement. It is not intended to serve as a definitive framework for the education sector's management of student data, nor is it intended to provide states with detailed guidance on implementation. Leaders and experts from the education, data, and privacy and security communities must work together to develop and implement such policies and practices.

Maximizing Data Investments While Minimizing Data Risks

To maximize investments in data systems, minimize data risks, improve data quality and increase data management efficiency, the education sector must ***achieve a common understanding of and commitment to privacy and security principles, address legal roadblocks*** preventing appropriate data use, and ***provide sensible implementation and oversight of strong policies and practices*** that protect student data from misuse.

Achieve a common understanding of and commitment to privacy and security principles

Over the last 40 years, industry leaders, policymakers, and privacy and security experts around the world have adapted and adopted a basic set of principles for safeguarding personally identifiable information. There is broad international agreement on the underlying substance of these principles, known as the Fair Information Practices (FIPs), and they have been adapted and adopted in various ways for different countries, contexts and sectors. (See the box below.)

Summary of Fair Information Practices (FIPs)

In 2011, the Obama administration released the *National Strategy for Trusted Identities in Cyberspace,* which included an expanded version of the FIPs summarized below. This version is unique in that it is endorsed by the White House and is intended to guide both private and public sectors.

1. **Transparency:** Be transparent and notify individuals regarding collection, use, dissemination and maintenance of personally identifiable information.
2. **Individual Participation:** Involve the individual in the process of using personally identifiable information and, to the extent practicable, seek individual consent for the collection, use, dissemination and maintenance of personally identifiable information. Organizations should also provide mechanisms for appropriate access, correction and redress regarding use of personally identifiable information.
3. **Purpose Specification:** Articulate the authority that permits the collection of personally identifiable information and specifically articulate the purpose or purposes for which the personally identifiable information is intended to be used.
4. **Data Minimization:** Only collect personally identifiable information that is directly relevant and necessary to accomplish the specified purpose(s) and only retain personally identifiable information for as long as is necessary to fulfill the specified purpose(s).
5. **Use Limitation:** Use personally identifiable information solely for the purpose(s) specified in the notice. Sharing personally identifiable information should be for a purpose compatible with the purpose for which the personally identifiable information was collected.
6. **Data Quality and Integrity:** To the extent practicable, ensure that personally identifiable information is accurate, relevant, timely and complete.
7. **Security:** Protect personally identifiable information (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. **Accountability and Auditing:** Be accountable for complying with these principles, provide training to all employees and contractors who use personally identifiable information, and audit the actual use of personally identifiable information to demonstrate compliance with these principles and all applicable privacy protection requirements.

In the United States, the FIPs are manifested in a number of formal and informal ways. For example, many federal laws draw on the FIPs, including the Privacy Act of 1974, the Family Educational Rights and Privacy Act (FERPA), and the Paper Work Reduction Act of 1980. Federal agencies have used the FIPs to develop sector-specific guidance. In 2010, a prominent public-private collaborative in the public health field produced a detailed and comprehensive set of practices to help protect the privacy and security of increasingly electronic personal health records and related services. Policymakers, education leaders and other stakeholders should be familiar with these principles and concepts and do their part to implement policies and practices to address them.

The education sector does not currently have a formally documented and broadly used version of the FIPs. However, the U.S. Department of Education (ED) is taking steps to proactively provide stakeholders technical assistance on these issues, including hiring a chief privacy officer; establishing a new Privacy Technical Assistance Center; and producing a series of technical briefs designed to guide state officials. The first brief in the series suggests that the education sector look to the FIPs as a "framework for a sound privacy and confidentiality data protection program" and describes how the FERPA statute and regulations address the principles. It remains to be seen if ED will directly formalize a set of FIPs for education.

Address legal roadblocks preventing appropriate data use in education

Maximizing states' investments in state longitudinal data systems will happen only if the right data get to the right people at the right time. This requires linking and sharing data across systems to produce better information, providing timely and appropriate access to stakeholders, and using data to conduct research and evaluation. Unfortunately, the lack of clear and consistent guidance from ED about how FERPA applies to states' authority to share and use longitudinal data in these ways has served as a roadblock to states' efforts. States have long requested clarifications on these issues to support their effective and appropriate use of data to meet their state goals and federal policy obligations while protecting data. In April 2011, ED proposed amendments to FERPA regulations; an initial analysis suggests that they would clarify much of states' confusion and foster a meaningful discussion about how to balance the effective use of data while protecting privacy.

Provide sensible implementation and oversight of strong policies and practices

The national conversation about the privacy, security and confidentiality of education data too often focuses exclusively on FERPA. While federal laws establish some broad parameters and guidance around rights, roles and responsibilities, states' development and implementation of policies and practices to manage data and data systems are where the rubber hits the road. Over the last two years, necessary attention has been brought to the policies and practices that states must develop and implement to ensure student data are properly managed to protect privacy, security and confidentiality. States are improving their efforts to be transparent about these policies and practices, and the DQC has developed several resources highlighting current states' policies and practices (see "Related DQC Resources").

State Policymakers' Responsibilities To Protect Student Information

State policymakers have three overarching and interconnected responsibilities to protect the privacy, confidentiality and security of student information:

- **Establish roles for data stewardship:** Define and clearly communicate authority, responsibility and accountability for decisionmaking, management and security of data

Within the state education agency, the chief information officer typically oversees data stewardship. However, this is not a one-person job; every stakeholder that "touches" or "uses" data — from the governor to the school secretary — has a role in protecting the privacy, security and confidentiality of student information. States must develop, document and communicate defined roles and responsibilities, including how challenging issues are escalated for resolution. These models will look a little different in each state and are called a variety of names: governance models, security programs, stewardship protocols, data use and access policies, etc. The state education agency must coordinate its effort with statewide laws, policies, information technology standards and protocols and may need to coordinate with other state officials, such as the state auditing agency or a chief information officer who has executive-level, statewide responsibility for information technology.

State policymakers are increasingly working to link or share K–12 data with appropriate data housed in systems managed by other agencies or entities (such as data from early childhood, postsecondary education and the workforce); this work is critical to ensuring states have the information necessary to answer key policy, programmatic and operational questions. State policymakers must leverage the collaborative power of cross-agency governance bodies to make decisions about sharing data across systems. Additionally, they must ensure all stakeholders understand their role in data stewardship and are aware of the danger and consequences of not fulfilling their responsibilities.

- **Ensure policy documentation, transparency and enforcement:** Document laws, policies and decisions related to data governance and communicate these policies and procedures in a way that is accessible to stakeholders, including agency staff, students, parents and the public

While states may have designed and implemented policies and practices to address privacy, security and confidentiality concerns, too often these documents are difficult to find, obtain and navigate. State policymakers are responsible for ensuring that proactive steps are taken to address these concerns. And external stakeholders, particularly students and parents, have a right to be informed about these policies and practices.

- **Support organizational capacity:** Ensure the state has the capacity and resources to implement and sustain these policies and procedures, including staff and technical system infrastructure

Data Stewardship Defined

In its recent brief, *Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records,* the National Center for Education Statistics defines data stewardship as "an organizational commitment to ensure that data in education records, including personally identifiable information:

- Are accurate, complete, timely, and relevant for the intended purpose;
- Are collected, maintained, used, and disseminated in a way that respects privacy and ensures confidentiality and security;
- Meet the goals of promoting access to the data for evaluating and monitoring educational progress and educational programs; and
- Meet the goals of assuring accuracy to ensure that decisions relating to an individual student's rights and educational opportunities are based on the best possible information."

State efforts to protect student data will be effective only when there is sufficient organizational capacity to oversee, manage and implement them. Protecting the privacy, security and confidentiality of student data involves technology, project management, data and security components and must take into account cultural, political and human considerations. This work is also iterative by nature: Policies and practices need to be consistently implemented and updated to keep pace with innovations in technology, new demands and risks, and best practice. State policymakers must ensure that the state has the necessary human, technical and financial resources to implement and sustain this work over time.

State Policies and Practices Designed To Protect Data

States policies and practices should maximize investments in data systems, minimize data risks, improve data quality and increase data management efficiency.

The table on page 5 describes a series of questions that state policymakers can use to navigate their conversations with staff, stakeholders and experts about these issues. Professionals in the data, security and information technology fields will recognize these considerations as minimum expectations, many of which are required by state or federal law and are inherently part of the design and implementation of statewide longitudinal data systems. While the detailed work of implementation will typically be led by agency professionals, state policymakers should be familiar with these concepts to meet their own responsibilities.

State Responsibilities and Critical Questions To Protect Student Data

Through a ***common understanding of and commitment to privacy and security principles, addressing legal roadblocks*** preventing appropriate data use, and ***providing sensible implementation and oversight of strong policies and practices*** that protect student data from harm, the education sector can maximize investments in data systems, minimize data risks, improve data quality and increase data management efficiency.

State policymakers have three overarching responsibilities to help protect the privacy, security and confidentiality of students' personally identifiable information.

Establish roles for data stewardship: Define and clearly communicate authority, responsibility and accountability for decisionmaking, management and security of data.

Ensure policy documentation, transparency and enforcement: Document laws, policies and decisions related to data governance and communicate these policies and procedures in a way that is accessible to stakeholders, including agency staff, students, parents and the public.

Support organizational capacity: Ensure the state has the capacity and resources to implement and sustain these policies and procedures, including staff and technical system infrastructure.

State officials responsible for the stewardship of student data and state data systems should ensure state policies and practices are designed to:

Justification	Justify that the student data being collected and stored are necessary, useful, accurate and valid	▶ Have you established a discrete set of policy, programmatic and operational needs that require the collection of student data? ▶ Have you documented how data collections align with these needs and the source of the requirement? ▶ Do you regularly review and update data collections to ensure only necessary data are collected? ▶ Have you established policies and procedures for regularly and securely archiving or destroying student records? ▶ Do you regularly audit data quality and accuracy processes?
Access	Limit access to personally identifiable information to necessary and appropriate individuals	▶ Have you defined multiple levels of access based on individuals' roles that limit the type of data individuals can access and for which students? ▶ Do you take the necessary steps to restrict access to personally identifiable information and to de-identify such information? ▶ Have you established internal procedural controls, including training and confidentiality agreements for staff who have access to data and mechanisms to track data access?
Sharing	Protect data that are shared from inappropriate use	▶ Have you established policies to guide decisions about whether to share data among state agencies, among postsecondary institutions, with researchers and with third-party contractors? ▶ When data are shared (including among state agencies, among postsecondary institutions, with researchers and with third-party contractors), are sharing agreements put in place to ensure confidentiality? ▶ When data are reported publicly in aggregate form, such as through state education agency websites or report cards, are the most robust methods used to protect personally identifiable information?
Security Framework	Implement a security framework that protects student information	▶ Have you developed a comprehensive security framework, including administrative, physical and technical procedures for addressing information technology, project management, data and security issues? ▶ Do you implement training, monitor compliance and regularly assess security operations? ▶ Have you established policies and procedures for crisis management, including data losses and security breaches?
Proactive Communication	Provide public and parental notice about data collection, policies, access and use	▶ Do you communicate with students, parents and the public about what information is being collected and shared and why? ▶ Do you annually notify students and parents about their rights under federal and state law, how they can access their student's information, and the processes to request changes to those data?

Related DQC Resources

- *Protecting the Privacy, Security and Confidentiality of Student Information: How States Can Maximize Data Investments and Minimize Data Risks* — A detailed analysis, additional background information and links to state examples and additional resources on this issue can be found in the DQC resource guide.
- *DQC Issue Page: Family Educational Rights and Privacy Act (FERPA)* — DQC's dedicated page for FERPA issues includes more information about its application to statewide data systems, including DQC analyses and commentary on the April 2011 proposed regulations.
- *Using Data To Improve Education: A Legal Reference Guide to Protecting Student Privacy and Data Security* — This resource provides summaries of multiple federal and state laws that have implications for statewide longitudinal data systems and can be accessed by federal law, state law by issue and state law by state (developed in partnership with Education Counsel, LLC, and Nelson Mullins Riley & Scarborough, LLP).
- *DQC Resource Library: State Policy Documents Documenting How States Protect the Privacy, Security and Confidentiality of Student Data* — DQC's web-based Resource Library warehouses a variety of resources published and produced by states, national organizations and federal agencies. In recent months, the DQC has added numerous state documents that describe states' policies and practices designed to protect the privacy, security and confidentiality of student data.
- *Call to Action: Clarify Application of FERPA to State Longitudinal Data Systems.* This statement notes four areas of ongoing confusion regarding the application of FERPA to state longitudinal data systems and calls on federal policymakers to address them.

References

- Education Counsel, LLC, *Advisory and Overview: U.S. Department of Education Proposed New FERPA Regulations,* www.DataQualityCampaign.org/files/Overview_FERPA_NPRM_EdCounsel.pdf.
- R. Gellman, *Fair Information Practices: A Basic History,* Version 1.82, April 19, 2011, http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.
- Markle, *The Markle Connecting for Health Common Framework for Networked Personal Health Information,* www.markle.org/health/markle-common-framework.
- National Center for Education Statistics, *Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records,* http://nces.ed.gov/pubs2011/2011602.pdf.
- National Center for Education Statistics, *Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records,* http://nces.ed.gov/pubs2011/2011601.pdf.
- U.S. Department of Education, *Safeguarding Student Privacy,* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/safeguarding-student-privacy.pdf.
- White House, *National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy,* www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

DATA QUALITY CAMPAIGN
Using Data To Improve Student Achievement
www.DataQualityCampaign.org

To download DQC resources, visit www.DataQualityCampaign.org, follow us on Twitter or visit us on Facebook.

The **Data Quality Campaign (DQC)** is a national, collaborative effort to encourage and support state policymakers to improve the availability and use of high-quality education data to improve student achievement. The campaign provides tools and resources that will help states implement and use longitudinal data systems, while providing a national forum for reducing duplication of effort and promoting greater coordination and consensus among the organizations focused on improving data quality, access and use.