**DQC Comments on the Posted Recommendations regarding Data Security and Privacy Protections**

The Data Quality Campaign (DQC) commends the U.S. Department of Education (the Department) for its efforts to highlight the need to ensure the security, privacy and confidentiality of sensitive education data and to provide more systematic assistance to states and local agencies in meeting these challenges. We appreciate the opportunity to provide feedback to the initial recommendations made to the Department by Highlight Technologies on issues related to data security and privacy protections.

The 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 DQC 10 Essential Elements of Statewide Longitudinal Data Systems have provided a broadly adopted framework for states[1]. From the outset of its work, the DQC Partners recognized that "[W]hile building and using these indispensable data systems are important for policy, management, and instructional decisions that focus on individual success, these needs must be balanced with appropriate protections for the privacy of student records."[2] In fact, in the DQC's inaugural publication released in 2005, the DQC highlighted privacy protections in its short list of System Fundamentals that states needed to address in addition to the 10 Essential Elements.

Protecting student privacy and data security requires strategic and deliberate action by stakeholders at all levels and positions of our education system. The current redoubled effort to ensure the security and privacy of identifiable information needs to highlight the different roles and responsibilities specific stakeholders must embrace for successful privacy protections.

The DQC Partners applaud the general intentions of the recommendations, and want to highlight that local and state leaders and stakeholders of education data need to be actively engaged in enacting and owning these actions. As a result of our initial analysis and interpretation of these recommendations, as well as conversations with privacy and security experts and state stakeholders, we offer four overarching reactions, as well as a handful of specific questions. We hope these comments are the beginning of ongoing and transparent conversation between the Department and the field on these issues.

First, the four overarching issues that arise from review of the recommendations:

1. **There is a need to raise awareness, facilitate an inclusive dialogue, and solicit feedback on these recommendations and related action.** The issues covered in these recommendations are critically important to the future of the use of data in education and warrant significant and robust conversation. We are concerned that there has not be enough attention paid to the recommendations, particularly by the state policymakers and staff that will be most affected by them. At the time that these comments were written, only a handful of individuals had posted comments on the Department's blog and since the names of the Expert Advisory Panel that were consulted are not being made public, we cannot be sure that necessary players in the field have been made aware of them. The DQC staff will continue to facilitate conversations around these recommendations, and is happy to collaborate with the Department on these efforts. However, we believe it is incumbent on the Department to facilitate significant conversation around these recommendations, particularly with state policymakers and other state leaders.

2. **These recommendations represent a possible expansion of the role of the federal government in protecting privacy and ensuring security of state data.** Addressing the privacy and security issues

[1] Data Quality Campaign, *Creating a Longitudinal Data System: Using Data to Improve Student Achievement,* http://dataqualitycampaign.org/files/Publications-Creating_Longitudinal_Data_System.pdf.
[2] Data Quality Campaign, *Maximizing the Power of Education Data while Ensuring Compliance with Federal Student Privacy Laws: A Guide for State Policymakers*, http://www.dataqualitycampaign.org/resources/details/32.

implicit in the use of data in education will likely require a mix of federal legislation and regulation; state legislation and regulation; industry commitment; and activity and support from external entities. Several of the recommendations include action by the Department in areas that may be outside the current capacity or historical role of the Department, or that may be more effectively implemented by other players.

This is not to be interpreted as saying these actions are unnecessary—in most cases we think the recommended actions are critical activities that must be addressed. It is also not meant to say that the Department should or should not do this work. Rather, we would like to see clarifications on the recommendation and further consideration of whether the Department is the entity best positioned to do this work or whether the recommended actions should be encouraged to be taken by states or other entities. As stated above, every stakeholder in the education system needs to take responsibility for ensuring the security and privacy of data; the question is what are the policy levers to ensure that the ownership of this issue is broadly adopted?

Below are a few examples of areas where the role of the federal government is not clear:

- *Providing guidance on managing breaches:* Given the fact that the majority of law on breaches exists at the state level, and that existing federal law and policy on breaches of education data are limited, it is not clear that the Department is best positioned to provide guidance to states on issues such as security breaches. Certainly states should be proactive in developing guidance related to their own policies that include addressing security breaches, and the expertise and authority relating to education and data appears to reside principally at the state level.

- *Developing a Leadership Dashboard to provide a snapshot on current privacy matter implementation status, gaps, and benchmark:* Typically, such monitoring and public communication of states' progress in improving specific areas of education policy is conducted by individual states and/or external, private entities. If the Department conducts this activity, it may be perceived as an enforcement strategy, federal audit, or precursor to sanctions that may compromise the utility of the activity in assisting states to make progress.

- *Developing recommended standards for security control; adaptation of the Federal Certification and Accreditation process; and certification of data systems:* It may be appropriate for the Department to proactively support the development of standards for security controls as recommendations for state implementation. However, what is the appropriate relationship between the setting of these voluntary standards and the government's authority to enforce them? Legislation likely would be required to provide this authority.

- *Working with International Association of Privacy Professionals (IAPP) to develop a professional certification program for privacy professionals in education:* Are there other cases where the federal government has worked with IAPP to develop the certifications? This action may be more appropriate to happen outside the context of the federal government.

3. **The recommendations do not do enough to reinforce and support state ownership and implementation of privacy and security policies and practices.** Addressing the highlighted and other issues of data security and student privacy will require significant action by state policymakers and state agency staff and their local counterparts. The recommendations note that the Department should develop training and professional development opportunities to build the capacity to address these issues. It is our understanding that the Department's new Privacy Technical Assistance Center is intended to provide a one-stop resource for state and local education agencies and the postsecondary community regarding data privacy, confidentiality, and security practices related to state longitudinal data systems.

   However, it will take significant capacity at the state level to actually implement policies and practices. What will the Department do to engage state policymakers to understand these issues, provide feedback to their activities and these recommendations, and discuss implementation concerns and challenges? Will

the Department consider other federal mechanisms for supporting states' efforts to address these issues, such as dedicated funding or inclusion of these activities in the requirements of the existing competitive Statewide Longitudinal Data Systems program? What legislative action, if any, is necessary to ensure that federal policies, such as the impending reauthorization of the Elementary and Secondary Education Act, reflect the recommendations that will result from the Department's activities?

It is critically important that the focus of our collective efforts be to improve state and local policies and practices.

4. **There remains a significant need for proactive federal administration of FERPA.** While many of the recommendations entail federal action in areas and roles new to the Department, proactive administration of the federal Family Educational Rights and Privacy Act (FERPA) is a definite responsibility of the Department that requires significant attention.

   Too often, conversations and policies related to privacy and security of education data have been limited to real and perceived FERPA barriers. State policymakers have asked continuously for clarification of how FERPA applies to state longitudinal data systems and how to align FERPA privacy protections with the need to use student information to improve student achievement and system performance, consistent with other federal mandates. These clarifications would not weaken privacy rules, but rather provide clarity to a confusing and outdated law. [3]

   DQC Partners have been vigorous advocates seeking federal clarification on FERPA, and applaud the Administration's current intention to craft new clarifying regulations and guidance that address these needs. Given the Department's responsibility for administering FERPA, we suggest that that effort must be among the highest priorities for the Department.

Additionally, the recommendations raise a number of specific issues we encourage the Department to address more thoroughly.

- *Is it feasible and/or appropriate to have the Department require "states and school systems . . . to come together…to agree upon what the specific purposes are for collecting student data?"* The intended purpose of this recommendation is unclear. The recommendations seem to indicate that the Department should require states and districts to collaborate on the articulation of a universal set of purposes for the collection of education data. This implies that the use of education data is a one-size-fits-all concept, the purposes of which can be decided collectively and at a single time. State data systems have been built by states for use by states and districts to meet their priorities. It seems more important that the Department encourage states and districts to conduct this activity regularly as part of their ongoing work to develop, govern, improve, and use their own data systems in the context of state and local education and policy needs. Also, does the recommendation apply to the Department's own data collections? Will the Department articulate specific purposes for each of its required data collections?

- *What is the role of notice and consent as articulated in the Fair Information Practice Principles (FIPP) in a comprehensive framework to guide education security and privacy practices?* The DQC agrees enthusiastically that it would be helpful to the education sector to have a broadly accepted framework to guide efforts to ensure there is an appropriate and effective balance between the use of data to improve student outcomes and the need to protect data security and student privacy.

  Certainly the FIPPs and their various applications are important reference statements that should inform that framework and help to guide its development. However, the FIPPs do not align perfectly with most United States federal or state laws on privacy and security, including FERPA, where most

[3] Education Counsel, *Needed Changes in FERPA Law, Regulations, or Guidance To Harmonize FERPA with the Functions of State Longitudinal Data Systems*, http://dataqualitycampaign.org/files/publication-needed_changes_ferpa_not_addressed_regulations-122808.pdf

issues applicable to state longitudinal data systems apply to situations where there is no parental or student consent. Also, there are alternative approaches that might inform the framework and focus on preventing and mitigating harm. We recommend that the Department facilitate a broader conversation around the range of principles that might be incorporated in a broadly accepted framework for education data.

- *What is the appropriate level of federal prescription around specific processes (such as around the wide variety of authentication processes necessary in education)?* Typically, security policies are developed through a risk analysis that considers the following sequence of questions: What is the information being stored? What is the risk of that information being inappropriately accessed or used? What is the necessary, appropriate, and reasonable authentication process to protect against that particular risk?

  The recommendations advocate that the Department encourage states' universal adoption of two-factor authentication processes, despite noted disagreement among the Expert Advisory Panel regarding the feasibility of implementing this approach. Also, while the recommendations note that there are many implementation options for two-factor authentication processes, they seem to recommend two specific processes.

  Were the recommendations intended to be interpreted as encouraging states' universal adoption of specific two-factor authentication processes for all remote access situations? If so, the Department may want to consider a different approach that encourages states to conduct risk analyses and develop and implement authentication processes in light of those findings and appropriate for their state-specific governance structures, the level of risk associated with the data to be accessed through that authentication, and other relevant facts and circumstances.

- *What is the goal of the recommendation that the Department research and report on interagency research agreements?* It is not clear what the goal or intention of the recommended action is. For example, is it to evaluate these agreements for FERPA violations? To identify a set of allowable purposes for interagency research agreements? To highlight the need for states to have these agreements in place?

- *What are the broader questions related to research on unique student identifiers with the purpose of discouraging the practice of using Social Security Numbers (SSNs)?:* If the Department is to take on such research, will it also consider the broader questions related to this issue? For example, any government-issued identification number is likely to have similar risks attached to it. What can be done to reduce those risks? Also, there is increased encouragement from the Department, particularly through the implementation of the American Recovery and Reinvestment Act (ARRA), to link K-12 data with workforce data—where SSNs are often the unique identifier. Will the Department provide guidance to states on how to link to workforce data systems that use SSNs while not using the SSNs as the unique student identifier? Many states have found such linkages to significantly improve match rates.

We commend the Department for its leadership in exploring these issues related to data security and privacy and the DQC Partners look forward to continuing this open and valuable dialogue.