PARCC Data Privacy & Security Policy
Executive Summary
December 2013

Overview

The PARCC states have developed a consortium-wide policy that lays out how PARCC and its contractors will work with states to comply with legal requirements regarding the protection of student data. The policy was drafted for PARCC by legal counsel from Education Counsel, LLC (and its affiliate, Nelson Mullins Riley and Scarborough LLP), and were reviewed by state assessment, data, contracts and legal staff.

States currently contract with assessment vendors to administer, score, and report results for their existing state assessment programs. In order to support the states' administration of the assessments, these vendors have access to a limited set of personally identifiable information (PII). Through contracts with those vendors and through other state policies, state education agencies set rules and policies that require vendors to protect the privacy and security of PII.

As states move to the PARCC consortium assessments, they will also provide limited access to PII to the contractors – just as they do now with their current testing programs and current assessment vendors. The PARCC policy is designed to provide states with rigorous protections necessary to ensure that PARCC and PARCC contractors:

- Only have access to personally identifiable student information as authorized in the agreement and data policy, or if further authorized by the state education agency to use that data for specified purposes; and
- Implement stringent policies and procedures to ensure the security of data and limit access to PII to only those employees who require it to conduct activities authorized by state education agencies.

Key Principles

The key principles that guide the policy are:

1. **States retain responsibility for and control over their data**. **Neither PARCC nor PARCC contractors will share student data with any outside entity, including the federal government.**

2. **States must give permission to PARCC and PARCC contractors in order for them to access any personally identifiable information – and only for specific purposes defined by states**.

3. **The policies and requirements apply not just to PARCC but to its PARCC contractors**.

These are foundational policies that will guide the way PARCC states conduct business with PARCC and the contractors delivering the PARCC assessments in 2014-15 and beyond. These policies will be incorporated into contracts with future PARCC contractors to ensure their compliance with the states' requirements.

Data Privacy & Security Policy

The Data Privacy & Security Policy includes a number of important provisions:

- Defines "personally identifiable information" as data that includes direct characteristics that would allow identification of a student (e.g., name, Social Security number) or indirect characteristics (e.g., small cell sizes), consistent with FERPA.
- Stipulates that state education agencies determine whether PARCC or PARCC Contractors have access to any PII.
- Establishes the purposes for which states would disclose PII to PARCC or PARCC contractors, which includes:
    - conducting research studies for states and districts to develop, validate, and administer assessments, and
    - assisting states in program evaluation and compliance with federal requirements (e.g., reporting student achievement results as required under ESEA).
- Sets basic privacy protections and limits on access to PII that states provide to PARCC or PARCC contractors, such as access rules and electronic data encryption requirements.
- Establishes key physical, administrative, and technical safeguards to ensure PARCC and PARCC contractors manage and control risks related to the availability and security of data – and ensure accountability for any breaches of security.
- Sets guidelines for the enforcement of this policy by PARCC and PARCC states, including disciplinary actions for employees of PARCC or PARCC contractors.
- Requires that PARCC designate a senior official to manage the policy and data agreements and establish a committee to monitor implementation of the policy, and that each member state designate a privacy administrator to oversee state functions under the agreement.

Together, these provisions establish a rigorous set of policies and procedures that will help states ensure the highest levels of security for student data.

Data Agreements

In the future, as a companion to the consortium's Data Privacy & Security Policy, states will ask PARCC and PARCC contractors to sign data agreements that set the terms under which they will share data for purposes authorized by the states.

The agreements are expected to include the following elements:

- Affirms that only individual states can authorize the use of student data by any outside organization that requests it from PARCC.
- Establishes the limited set of allowable uses for student data by PARCC and the terms under which that data will be provided by states to PARCC.
- Outlines the limited conditions under which PARCC can use PII in studies approved by state education agencies.
- Sets administrative, technical, and physical data privacy and security controls for PARCC and PARCC contractors, such as requiring contractors to abide by all policies set by PARCC and accounting for the appropriate destruction of all PII when the information is no longer needed for PARCC services to a member state (or when requested by the state).