PARCC
Partnership for Assessment of Readiness for College and Careers

PARCC Data Privacy & Security Policy

Adopted by the PARCC Governing Board

December 2013

Table of Contents

I. Introduction

Ii. Definitions

Iii. Privacy of Personal Information

A. Basic Privacy Protections

B. Access to PARCC PII

Iv. Information Security Program

A. Information Security Risk Assessment

B. Security Controls Implementation

C. Security Monitoring

D. Security Process Improvement

E. Breach Remediation

F. Organization, Responsibilities and Administration

G. Personnel Security Policy Overview

V. Enforcement

I. INTRODUCTION

Purpose and Approach. The Partnership for Assessment of Readiness of College and Careers ("PARCC") is a non-profit consortium of states that have organized themselves to develop new assessment systems that measure student knowledge and skills against a common set of college- and career- ready standards in mathematics and English language arts in a way that covers the full range of those standards, elicits complex student demonstrations or applications of knowledge and skills, as appropriate, and provides an accurate measure of student achievement across the full performance continuum and an accurate measure of student growth over a full academic year or course. This effort is managed by PARCC, Inc., a non-profit organization created by the consortium. In addition, individual states that are members of the consortium obtain services to develop and implement their assessment systems from contractors that are engaged through the consortium, for example, by "piggy-backing" on or joining contracts awarded by a lead state in the consortium, or by awarding their own contracts to these contractors.

Use of Personally Identifiable Information. Personally Identifiable Information ("PII") on students, including information on their performance on the assessments and limited student demographic information,[1] will be provided to these contractors by states and may also be provided to PARCC, Inc. and PARCC, Inc.'s contractors as necessary to develop and implement the assessment systems. (PARCC, Inc.'s contractors and the contractors of member states engaged through the PARCC Consortium are collectively referred to in this policy as the "PARCC Contractors.") The PII will be provided by member states or their local education agencies. PII will never be provided by PARCC to the federal government without written authority from a state, or unless legally required to do so by subpoena or court order. Disclosure of PII to PARCC and its contractors is authorized by the Family Educational Rights and Privacy Act ("FERPA") only for the purposes of—

(1) Conducting studies, for or on behalf of participating states and their local education agencies, to develop, validate, and administer predictive tests or to improve instruction (34 CFR 99.31(a)(6)(i)(A) & (C)); and

(2) Assisting in the evaluation of federal- and state-supported education programs and ensuring compliance with federal legal requirements related to such programs – in particular related to state-level assessments and accountability systems (34 CFR 99.31(a)(3) & 99.35).

More specifically, the data will be used by one or more of the PARCC Contractors or by PARCC, Inc.—

[1] For example, states and districts currently collect information about students' gender, race/ethnicity, and free/reduced lunch status in order to report disaggregated assessment results to schools, districts, families, and the public.

- to validate, pilot and field test, and improve the assessments;

- to report assessment results back to states and their local education agencies in a form that is useful to them;

- to prepare reports on student performance for participating states, their local education agencies, and the public (PII may not be included in public reports or in reports to states or local education agencies that were not the source of the PII);

- to analyze test results to assist member states and their local education agencies for purposes of accountability, including promotion and graduation decisions for individual students; teacher and school leader evaluations; school accountability determinations; determinations of principal and teacher professional development and support needs; and teaching, learning, and program improvement; and

- to carry out studies designed to improve instruction on behalf of participating states and their local education agencies, pursuant to separate agreements with the member states and/or their local education agencies.

State and Local Education Agency Ownership of the Data. Access to student data provided to PARCC Contractors or PARCC, Inc. remains the legal responsibility of participating states and their local education agencies, in accordance with FERPA and applicable state law, and member states or their local education agencies maintain ownership of these data. These data shall not be used for commercial purposes, nor shall PARCC or PARCC contractors share personally identifiable information with the federal government, unless legally required to do so by subpoena or court order. The principles described in this paragraph apply not just to PII, but to all data provided by the state or its local education agencies. However, the requirements and policies in this Data Privacy and Security Policy apply specifically to the use and protection of PII provided by the state educational agency or its local education agencies.

Purpose/Application of this Policy. This Policy describes, in general, (i) what steps must be taken to protect PII that is accessed by or provided to PARCC Contractors or PARCC, Inc.; (ii) how that information is used; (iii) with whom PARCC Contractors or PARCC, Inc. shares that information, and (iv) the steps PARCC Contractors or PARCC, Inc. take to protect the security of that information. This Policy also describes briefly the responsibility that member state educational agencies have for controlling access to the information maintained by PARCC Contractors or PARCC Inc.

This Policy has been developed with the input of member states, which also will have the opportunity to review amendments to the Policy. Monitoring of the implementation of this Policy is the responsibility of a PARCC Committee on Data Management, Privacy, and Security. Enforcement of this Policy is a critical responsibility of PARCC, Inc. and its Chief Executive Officer.

Each of the privacy and security provisions in this Policy is effective as of the Effective Date set forth in the Policy and applies to PARCC, Inc., PARCC Contractors, and, where applicable by its terms, to member state educational agencies and their employees that have access to PII through PARCC, Inc. or PARCC Contractors.

The privacy and security provisions in this Policy do not generally apply by the terms of this Policy to participating state educational agencies, but do apply to state educational agency contracts entered into by member states through the PARCC Consortium. Each participating state educational agency is responsible for ensuring its own compliance with applicable law, including FERPA. Accordingly, member state educational agencies determine what privacy and security requirements to establish for themselves and may elect to adopt all or some of the provisions in this Policy. However, member state educational agencies are obligated to include the privacy and security requirements in this Policy in contracts with contractors engaged through the PARCC Consortium. To the extent that certain provisions in this Policy are not by their terms applicable to participating state educational agencies, such state educational agencies also may elect to apply all or some of such provisions in this Policy to themselves and their own employees.

Protection of Social Security Numbers. In order to protect against the danger of identity theft and to increase the confidentiality of the data transmitted in accordance with this policy, no State Educational Agency or local education agency will disclose Social Security numbers to PARCC, Inc. or to PARCC Contractors.

II. DEFINITIONS

Capitalized terms referenced herein but not otherwise defined shall have the meanings as set forth below:

“Authorized User” means an individual employee or contractor of a state educational agency authorized by such state educational agency to access PII maintained by PARCC, Inc. or PARCC Contractors.

“Breach” means the unauthorized acquisition, access, use, or disclosure of PII which compromises the security or privacy of such information.

"Destroy" or "Destruction" means the act of ensuring the PII cannot be reused or reconstituted in a format which could be used as originally intended and that the PII is virtually impossible to recover or is prohibitively expensive to reconstitute in its original format.

“FERPA” means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and its implementing regulations, as they may be amended from time to time. The regulations are issued by the U.S. Department of Education, and are available at http://www2.ed.gov/policy/gen/reg/ferpa/index.html.

"PARCC Contractor" means each contractor of PARCC, Inc. that may be required to maintain or handle PII in the course of providing services in support of member states and each contractor engaged by a member state through the PARCC Consortium – i.e., by joining a contract awarded by a lead state in the consortium, or by awarding its own contract to a contractor selected by another member state to provide services for purposes addressed by the consortium – that may be required to handle such data in the course of providing services to the member state.

"Personally Identifiable Information" (or "PII") means any information defined as personally identifiable information under FERPA or relevant state law, including small cell-size data that are linkable to a specific student, as provided under FERPA regulations. PII includes, but is not limited to—

- The student's name;
- The name of the student's parent or other family member;
- The address of the student or student's family;
- A personal identifier, such as a student number;
- Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; or
- Other information that alone or in combination is linked or linkable to a specific student that would allow a reasonable person in the school community who does not have knowledge of the relevant circumstances, to identify the student with reasonable certainty.

As noted in the introduction, "Personally identifiable Information" (or "PII") does not include Social Security numbers, which may not be disclosed to PARCC, Inc. or to PARCC Contractors.

"Security Incident" is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices or an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies.

"Student Demographic information" means information required for disaggregated reporting of assessment results (such as economically disadvantaged students, students from major racial and ethnic groups, etc.), as provided under Section 1111(b)(3) of the Elementary and Secondary Education Act, as amended.

III. PRIVACY OF PERSONAL INFORMATION

A. Basic Privacy Protections

1. Compliance with Law and Policy. All PII uploaded to or made accessible to PARCC, Inc. or to PARCC Contractors will be handled, processed, stored, transmitted and protected in accordance with all applicable federal data privacy and security laws (including FERPA), data privacy and security laws of the state from which the data originated, and with this Policy.

   Each member state, in signing a data agreement with PARCC, Inc. warrants that (a) the data privacy and security provisions of this Policy comply with its state law and (b) it will promptly notify PARCC, Inc. and PARCC Contractors in writing of any changes in state law that affect the provisions of this Policy.

2. Training. Employees of PARCC, Inc. (including temporary and contract employees) and the employees (including temporary and contract employees) of a PARCC Contractor are educated and trained on the proper uses and disclosures of PII and the importance of information privacy and security. Such training will include training for new employees and refresher training for current employees.

3. Personnel Guidelines. All PARCC, Inc. employees and PARCC Contractor employees are required to be aware of and work to protect the confidentiality, privacy, and security of PII. PARCC, Inc. and the PARCC Contractors and their respective employees shall not access PII except to comply with a legal obligation under federal or state law, regulation, subpoena, or action by a member state educational agency that requires such access, or where they have a legitimate need for the information to maintain their data system or perform services for member state educational agencies as agreed upon in a data agreement between PARCC, Inc. and member states or in a data agreement with PARCC Contractors. The following list provides a general description of the internal policies with which PARCC, Inc. and PARCC Contractors and their respective employees are required to comply:

   a. Limit internal access to PII to PARCC, Inc. or PARCC Contractor employees with proper authorization and allow use and/or disclosure internally, when necessary, solely to employees with a legitimate need for the PII to carry out the educational purposes of PARCC, Inc. and PARCC Contractors pursuant to their MOUs or data agreements with member states.

b. Allow access by parties other than the state educational agency or local education agencies from which the PII was obtained to PII residing in PARCC, Inc. or PARCC Contractors only where users are authorized to have access to PII by the state educational agency for the state from which the PII was obtained.

c. Require that materials containing PII in electronic form are stored solely within encrypted data repositories and PII are not available on unencrypted shared drives that are used by other users or on a local drive.

d. When PII is no longer needed or states request the return of PII, delete access to PII, in accordance with secure Destruction procedures that the PARCC Governing Board and PARCC Committee on Data Management, Privacy, and Security has approved.

e. Permit PARCC, Inc. employees and PARCC Contractors to download information from PARCC onto storage only as directed by a participating state educational agency and verify and create a written record for retention by the participating state educational agency subject to audit that the information is encrypted and stored in password-protected files, and that devices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).

f. Require that any downloaded materials consisting of PII remain in the United States.

g. Prohibit the unencrypted transmission of information from PARCC, Inc. or PARCC Contractors, to any third party wirelessly or across a public network.

B. Access to PARCC PII

1. State educational agencies determine access to PII. Member state educational agencies that provide – or whose local education agencies provide -- access to PII to PARCC, Inc. or PARCC Contractors determine access to PII for parties beyond PARCC and PARCC Contractors and their employees. Member state educational agencies execute data agreements with PARCC, Inc. and with contractors that they select to engage through the PARCC Consortium which include requirements to comply with this Data Privacy and Security Policy, FERPA, and state law.

2. Parent Inquiries. PARCC, Inc. and PARCC Contractors shall cooperate with the state educational agency in addressing inquiries or complaints from parents (or students 18 and over) that relate to their use or disclosures of the PII. PARCC states shall agree to a set of decision rules that establish which types of inquiries member state educational agencies must handle and which PARCC, Inc. is responsible for handling.

3. Privacy Administrators. Each member state educational agency must designate a privacy administrator who is responsible for managing access to PII maintained by PARCC, Inc. or PARCC Contractors by designating authorized users, including employees of the state educational agency, and for determining the scope of PII to which they have access. If PII is provided to PARCC, Inc. or PARCC Contractors directly by local education agencies, the Privacy Administrator shall be responsible for coordinating requests to access local education agency data with the relevant local education agency. The Privacy Administrator shall be responsible for making all administrative decisions regarding access to and use of PII provided by the Privacy Administrator's agency to PARCC, Inc. or PARCC Contractors and shall be responsible for reviewing and approving access to the PII by categories of PARCC, Inc. or PARCC Contractor employees based on their need for such access to provide services under the state's data agreements with PARCC, Inc. or PARCC Contractors. A Privacy Administrator may delegate all or some of his or her functions under this Policy to employees within the state educational agency. It is the responsibility of the Privacy Administrator to ensure that authorizations to access PII are kept current regardless of cause. For example, when an employee of a state educational agency or of its contractor leaves that employment, all access to PII for that employee must be terminated.

IV. INFORMATION SECURITY PROGRAM

The security of the PII that state educational agencies provide to PARCC, Inc. or to PARCC Contractors is of critical importance to PARCC. PARCC's IT Security Program consists of technical, physical and administrative safeguards to protect the PII. PARCC's IT Security Program is designed to identify, manage and control the risks to system and data availability, integrity, and confidentiality, and to ensure accountability for system actions. PARCC's Security Program includes, and the security program of each PARCC Contractor is required to include, the following key general processes which may be more fully described in other materials as necessary:

A. Information Security Risk Assessment

PARCC, Inc. periodically conducts, and PARCC Contractors are required to periodically conduct, an accurate and thorough external assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing PII maintained by PARCC, Inc. and PARCC Contractors; to report such risks as promptly as possible to PARCC, Inc.'s Chief Executive Officer or other official within PARCC, Inc. designated to be responsible for data privacy and security compliance, or to the PARCC Contractor's CEO or designee, who in turn shall report such risks to PARCC, Inc's Chief Executive Officer or designee; and to implement security measures sufficient to reduce identified risks and vulnerabilities. PARCC, Inc.'s Chief Executive Officer or designee shall promptly report such risks to member states. Such measures shall be implemented based on the level of risks, capabilities, and operating requirements. These measures must include as appropriate and reasonable the following safeguards:

1. Administrative Safeguards

    1. Sanctions: Appropriate sanctions against PARCC, Inc. and PARCC Contractor employees who fail to comply with PARCC security policies and procedures, with the potential for criminal referral if warranted.

    2. System Monitoring: Procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.

    3. Security Oversight: Assignment of one or more appropriate senior officials within PARCC, Inc. and each PARCC Contractor, as applicable, to be responsible for developing, implementing, and monitoring of safeguards and security issues.

    4. Appropriate Access: Procedures to determine that the access of PARCC, Inc. and PARCC Contractor employees to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for PARCC, Inc. and PARCC Contractor employees who have access to PII.

    5. Employee Supervision: Procedures for regularly monitoring and supervising PARCC, Inc. and PARCC Contractor employees who have access to PII.

    6. Access Termination: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.

7. Recording Requests and Disclosures: Disclosures of PII to, and requests for disclosures of PII from, third parties -- other than employees of PARCC, Inc. or of a PARCC Contractor or the state educational agency or its local education agencies that provided the PII -- are recorded by the state educational agency.

2. Physical Safeguards

1. Access to PII: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.

2. Awareness Training: On-going security awareness through training or other means that provide PARCC, Inc. and PARCC Contractor employees (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training should also address procedures for monitoring log-in attempts and reporting discrepancies, as well as procedures for safeguarding passwords.

3. Incident Response Plan: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.

4. Physical Access: Procedures to limit physical access to PII and the facility or facilities in which they are housed while ensuring that properly authorized access is allowed, including physical barriers that require electronic control validation (e.g., card access systems) or validation by human security personnel.

5. Physical Identification Validation: Access is physically safeguarded to prevent tampering and theft, including procedures to address control and validation of a person's access to facilities based on his or her need for access to the PII.

6. Operational Environment: Procedures that specify the proper functions to be performed, the manner in which they are to be performed, and the physical attributes of the surroundings of facilities where PII is stored.

7. Media Movement: Procedures that govern the receipt and removal of hardware and electronic media that contain PII into and out of a facility.

8. Encryption and Final Disposition of Information: Procedures addressing encryption of all data at rest and in transit and the final disposition of PII. Procedures must include processes for the continued encryption of a state educational agency's PII through the time when its secure deletion/destruction has been requested by the state educational agency, or when the terms of the data agreement between PARCC, Inc. or a PARCC Contractor and a state educational agency require that the PII be deleted/destroyed.

3. Technical Safeguards

1. Data Transmissions: Technical safeguards to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups. Encryption shall be used when PII are in transmit or at rest. Unencrypted PII shall not be transmitted over public networks to third parties.

2. Data Integrity: Procedures that protect PII maintained by PARCC, Inc. or a PARCC Contractor from improper alteration or destruction. These procedures will include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.

3. Logging off Inactive Users: Inactive electronic sessions shall be designed to terminate automatically after a specified period of time.

B. Security Controls Implementation

PARCC, Inc. and PARCC Contractors will develop procedures addressing the acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the need for management and staff to understand their responsibilities and have the knowledge, skills and motivation necessary to fulfill their duties.

C. Security Monitoring

In combination with periodic security risk assessments, PARCC, Inc. and PARCC Contractors will use a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis. PARCC, Inc. and PARCC Contractors will also assess on an ongoing basis whether controls are effective and performing as intended, including intrusion monitoring and data loss prevention.

D. Security Process Improvement

Based on PARCC, Inc.'s and PARCC Contractors' security risk assessments and ongoing security monitoring, PARCC, Inc. and PARCC Contractors will gather and analyze information regarding new threats and vulnerabilities, actual data attacks on PARCC, Inc. and PARCC Contractors, and new opportunities for managing security risks and incidents. PARCC, Inc. and PARCC Contractors will use this information to update and improve their risk assessment strategy and control processes.

E. Breach Remediation

PARCC, Inc. and PARCC Contractors strive to keep PII maintained by PARCC, Inc. or a PARCC Contractor secure and to use reasonable administrative, technical, and physical safeguards to do so. PARCC, Inc. and PARCC Contractors will maintain and update incident response plans that establish procedures to follow in case a Breach occurs. PARCC, Inc. and PARCC Contractors will also identify individuals within their respective organizations responsible for implementing incident response plans if a Breach should occur.

Almost all U.S. states and other jurisdictions have laws requiring businesses to notify individuals in the event of any unauthorized acquisition of or access to files or documents containing such individuals' PII. State laws vary as to the types of PII that are covered, the methods of notification and the required contents of the notice, and whether notification is required when the PII is encrypted. Some states require notification to various third parties, such as law enforcement agencies, state attorneys general and/or credit reporting companies.

If PARCC, Inc. or a PARCC Contractor determines that a Breach has occurred, PARCC, Inc. or the PARCC Contractor, as applicable, will notify affected parties as promptly as possible, including participating state educational agencies and local education agencies that have directly provided the PII, and will cooperate with state educational agencies or such local education agencies as needed to enable compliance with all state breach of confidentiality laws. The breaching party will be liable for all costs associated with the breach.

PARCC, Inc. employees and PARCC Contractors are required to report as promptly as possible to the PARCC Chief Executive Officer (or his or her designee) and persons responsible for managing their respective organization's incident response plan any incident or threatened incident involving unauthorized access to or acquisition of PII of which they become aware. Such Security Incidents include any breach or hacking of the PARCC electronic data system or any loss or theft of data, other electronic storage, or paper. As used herein, "Electronic Data System" means all information processing and communications hardware and software employed in PARCC Inc.'s or the PARCC Contractor's business, whether owned by PARCC, Inc. or the PARCC Contractor, or

operated by its employees or agents in performing work for PARCC, Inc. or the PARCC Contractor.

Further, member state educational agencies are responsible for notifying PARCC, Inc. or PARCC Contractors, as applicable, as promptly as possible upon having any reason to believe that PII may have been lost, stolen, inappropriately accessed in or through PARCC, Inc. or a PARCC Contractor, or have been otherwise compromised.

F. Organization, Responsibilities and Administration

PARCC, Inc. will appoint and PARCC, Inc. or the member state, as applicable, will require that each PARCC Contractor appoint one or more senior officials responsible for developing, implementing and maintaining the Data Privacy and Security Program required under this Policy, under the oversight of PARCC Inc.'s or the PARCC Contractor's Chief Executive Officer and Governing Board, as applicable.

G. Personnel Security Policy Overview

PARCC, Inc. and each PARCC Contractor shall mitigate the risks posed by users of PARCC, Inc- or PARCC Contractor-maintained PII by:

1. Performing appropriate background checks and screening of new PARCC, Inc. and PARCC Contractor employees, in particular those who will have access to PARCC, Inc.- or PARCC Contractor- maintained PII;

2. Obtaining agreements from PARCC, Inc. and PARCC Contractor internal users covering confidentiality, nondisclosure and authorized use of PII; and

3. Providing training to support awareness and policy compliance for new hires and annually for all PARCC, Inc. and PARCC Contractor employees.

V. ENFORCEMENT

PARCC, Inc. and each PARCC Contractor will consistently enforce this Policy with appropriate discipline for its own employees. PARCC, Inc. and each PARCC Contractor, as applicable, will determine whether violations of this Policy have occurred and, if so, will determine the disciplinary measures to be taken against any director, officer, employee, agent or representative who violates this Policy.

The disciplinary measures may include counseling, oral or written reprimands, warnings, probation or suspension without pay, demotions, reductions in salary, or termination of service or employment, as well as criminal referral to law enforcement, if appropriate.

Persons subject to disciplinary measures may include, in addition to the violator, others involved in the wrongdoing such as (a) persons who fail to use reasonable care to detect a violation, (b) persons who withhold material information regarding a violation, and (c) supervisors who approve or condone the violations or attempt to retaliate against employees or agents or representatives of PARCC, Inc. or the PARCC Contractor for reporting in good faith violations or violators.

PARCC, Inc. or the state member, as applicable, also may take appropriate actions authorized under contract or by law regarding PARCC Contractors that fail to comply with the terms of this Policy. It is noted that if the U.S. Department of Education finds that PARCC, Inc. or a PARCC contractor has violated FERPA requirements related to disclosure, PARCC or the PARCC Contractor, as applicable, may be debarred by the U.S. Department of Education from access to PII from the state educational agency or its local education agencies for at least 5 years. PARCC, Inc. and PARCC Contractors are also accountable to each member state for compliance with this policy.