



COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF EDUCATION

House Education Committee
Hearing on Student Data Protection, Retention and Safety Procedures
October 24, 2022

Good morning, Chairman Sonney, Chairman Longietti, and honorable committee members. I am Julie Kane, Director of Policy and Planning at the Pennsylvania Department of Education (Department), and joining me today is David Ream, Director of our Office of Data Quality, to discuss student data privacy at the state level.

Access to the right kinds of information for those who need it is critical to ensuring success of the next generation of Pennsylvanians. From teachers supporting their students through personalized interventions in the classroom to business leaders trying to determine whether there will be an adequate supply of skilled employees for a new manufacturing plant, having the right data makes all the difference. But with access comes great responsibility, which the Department takes very seriously.

Pennsylvania has collected data and built a sophisticated infrastructure around data quality and reporting to fulfill state and federal reporting requirements for more than a decade. The central data repository is called the [Pennsylvania Information Management System \(PIMS\)](#), and it serves as Pennsylvania's statewide longitudinal data system for education data. PIMS serves several purposes:

- Meeting current state and federal reporting requirements;
- Improving education decision-making using high quality data and decision support tools;
- Providing longitudinal tracking of education progress over time and across local education agencies (LEAs); and
- Reporting timely and accurate education data through standardized and ad hoc reporting capabilities.

PIMS serves as the primary source of data for the Department required reporting and provides Pennsylvania education stakeholders—the governor, agency leadership, legislators, school district personnel, taxpayers, parents, and the community—with essential data to make sound decisions about education in the Commonwealth. PIMS was implemented in 2006 through a federal grant and continues to be supported through federal and state funding, both of which have been instrumental in expanding PIMS, guiding improved data use statewide, and implementing data safeguards.

Individual student data are managed in accordance with state and federal laws. The Family Educational Rights and Privacy Act of 1974 (FERPA), 20 U.S.C. §1232g, and its implementing regulations found at 34



COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF EDUCATION

CFR Part 99, the Individuals with Disabilities Education Act (IDEA), 20 U.S.C. §1417(c), 1439(a)(2), and its implementing regulations found at 34 CFR § 300.123 and §300.622, and Pennsylvania statutes, regulations and policies govern the confidentiality of, and access to, students' educational records.

To ensure the maintenance of confidentiality of student data, the [PDE Data Access and Use Policy](#) includes four privacy and confidentiality protections: assignment of a unique identifier, statistical security, data security, and restricted access.

Assignment of a Unique Identifier (PAsecureID)

The [PAsecureID](#) is a 10-digit number that is generated for each student, is unique to that student and protects the confidentiality of the individual student record of each student. The PAsecureID database contains a selected set of data about individual students that will allow for the assignment of a unique student identifier. The PAsecureID is randomly generated and contains no embedded meaning. Once the number is created it is first checked for duplicates. If any duplicates are found, they are reconciled using a set of information, such as the first name, last name, date of birth, gender, race/ethnicity, and the LEA identification number of the student. After being checked for duplicates, the number is made permanent. PAsecureID allows students to be anonymously identified without social security numbers.

The Department does not release or disclose personally identifiable student level data regarding students in the public schools of Pennsylvania unless permitted by law. Confidential data includes personally identifiable information about a student that is prohibited from disclosure pursuant to state or federal law or information that is intended for the use of a particular person/group and whose unauthorized disclosure could be prejudicial to the individual it identifies. Except in very limited circumstances set forth in 34 C.F.R. §99.31, information that allows for the identification of an individual student and that is collected by the Department is considered personally identifiable information and may not be released without parental consent. This information includes but is not limited to:

- Family information such as names, address, phone numbers, personal and business financial data, household members' social security numbers, household members' employment information, household Temporary Assistance for Needy Families (TANF), and Food Stamp eligibility;
- Personal information such as identification codes, grades, scores, courses taken, and other specific information linked directly to a student;
- Special Education records;



COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF EDUCATION

- Free or Reduced-Price eligibility status of individual students in USDA-funded school lunch, breakfast and milk programs, Summer Food Service Programs, and Child and Adult Care Food Programs; and
- Information that would make the student's identity easily traceable.

Statistical Security

The Department uses student data to produce aggregate reports that relate to groups of students, rather than individual students. While it may seem that the use of anonymous aggregated data poses little threat to confidentiality, there are some cases where specific populations may include only a few individuals. Statistical disclosure is the risk that arises when a population is so narrowly defined that tabulations are apt to produce a reported number small enough to permit the identification of a single individual. In such cases, the Secretary of Education will enforce statistical cutoff procedures using a minimum confidentiality n of 10 to ensure that student confidentiality is maintained. It is the intent of Department to avoid the possibility of inadvertently reporting personally identifiable information about any student.

Data Security

Security includes the technical measures that ensure records are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. Since the data are stored on computers, there are high levels of protection that provides integrity and availability commensurate with the level of risk and magnitude of harm. Procedures include secure firewalls, secure socket layers, audit trails and physical security, such as restricted server room access. All Commonwealth and federal security policies are followed and regularly audited.

Restricted Access to Student Data

The chief school administrator or their designee is responsible for authorizing access to data concerning students enrolled in that LEA. An individual is granted access to specific data in PIMS upon signing an assurance statement and receiving approval of the chief school administrator. LEAs are only allowed to view or download their own files. LEA staff may only use the search functionality for the purpose of locating students already assigned a PAsecureID. Department staff have access to student data on an individual basis only through a PAsecureID. The Department's Data Base Administrator has access to the entire database, but only for purposes of troubleshooting and correcting errors or avoiding potential errors. Any Department employee or authorized agent assigned responsibilities that require access to student data must sign an assurance statement. The level of access depends upon the staff member's responsibilities. Other staff only have access to aggregate data.



COMMONWEALTH OF PENNSYLVANIA
DEPARTMENT OF EDUCATION

PIMS data is provided to approved, qualified researchers in conformance to the [PDE Data Access and Use Policy](#) and FERPA. Only authorized individuals are granted access to the data. These authorized individuals may include Department personnel, contracted researchers, and researchers with a research study approved by the Department's Institutional Research Board (IRB). All authorized individuals must adhere to the dictates of the data sharing agreement for the specific data request and the [PDE Data Access and Use Policy](#). A [multi-tiered review process](#) ensures research applications, researchers and the data being requested are carefully reviewed and vetted. Once a research project receives IRB approval, researchers must enter a [data access agreement](#), which guarantees the data provided by PDE is protected. Researchers may not share data with anyone outside of the agreement, and all data must be destroyed after completion of the research project and in accordance with the timeframe agreed upon in the data access agreement.

The Department has a comprehensive toolset for educators and administrators to assist with issues of data quality and analysis. This toolset includes the [Pennsylvania Data Quality Curriculum](#) offered to educators annually at the [PDE Data Summit](#); the PIMS Data Quality Engine; the [Pennsylvania Data Quality Network](#); and technical assistance provided by intermediate units through the Department's State System of Support. These initiatives significantly strengthen the ability of schools to collect, access and share timely and accurate data in PIMS, and help teachers and school administrators understand the importance of safely maintaining data and data systems.

We appreciate the opportunity to speak with the Committee today on this important issue and welcome your questions.