Testimony on Student Data Retention and Protection

Pennsylvania House of Representatives Education Committee Hearing on October 24, 2022

Good morning Chairman Sonney, Chairman Longietti, and distinguished members of the House Education Committee. My name is Dr. Robin Felty, Superintendent of the Manheim Township School District. Also, with me today is Mr. Dan Lyons, Director of Technology Services at Manheim Township. Thank you for the opportunity to speak to you today on the important topic of student data retention, protection and overall security protocols. Manheim Township is located in Lancaster, serving approximately 6,000 students in 9 different schools – 6 elementary, 1 intermediate, 1 middle school and 1 high school.

The use of student data is an integral part of the learning process in schools today as it provides an opportunity to personalize and improve each student's learning. Data allows schools to target student instruction, as well as provides real-time feedback on student progress for teachers to customize instructional resources and time.

Having student data, however, comes with the responsibility to ensure that the data is appropriately secured, protected, and retained, and is consistent with applicable state and federal laws. Schools must utilize necessary firewalls, security certificates, and limitations on access to ensure that only people with a need have access to the data.

The types of student data are wide-ranging and falls under many different categories.

- The most valuable of that data is related to student demographics: full legal names, addresses, phone numbers, date of birth, current photo, and other items of this nature.
- In addition to demographic information, there is also much more sensitive data: economic status (free/reduced lunch), medical documentation, insurance information, disciplinary records, and family relationship identifiers (siblings or other school-age household members). There may also be legal information

associated with a student, such as a custody agreement between separated parents, adoption paperwork, immigration/naturalization tracking, or "homeless" status.

- A wealth of academic data exists for every student. Beyond the obvious courses and grades, there will be academic transcripts from previous schools, attendance records, truancy letters, transportation information, and more.
- For students who have been identified as needing special education services or other special services, their designations and associated documentation will also be tracked.

The bulk of student data is retained in the "Student Information System (or "SIS). For some districts, the SIS is a monolithic solution with all general education, special education, health services, and assessment tracking housed under a single application. For other districts, there may be several separate applications that comprise this overall "SIS" functionality. Additional data may also reside in electronic format in Technology Infrastructure such as Microsoft Active Directory, a Learning Management System such as Schoology or Canvas, a Single-Sign-On or Rostering Solution such as Classlink, or an individual application that may be used for diagnostic assessments or instructional content in many different subject areas.

Student Data is retained on varying timelines, dependent upon the nature of the data. Many records are retained only until the conclusion of each academic year, at which point they are deleted or destroyed. Student email is typically retained for a period of 3 years. The majority of additional data is typically retained for 6 years following the conclusion of a student's enrollment in the district (withdrawal or graduation). Some specific types of student data are subject to other retention periods, as governed by state or federal law. For example, a Sexual Harassment or Title IX Investigation Record is explicitly retained for 7 years, regardless of student enrollment status. In general, data of this nature is not stored in the Student Information System ("SIS"), so safeguards must be in place to ensure that paper or electronic records of this nature are handled appropriately and destroyed upon their designated "expiration date."

The exact methods of data security will vary depending upon the location of the data (on-premises vs. "the cloud"), the format of the data, and the platforms through which this data must be accessed. Some of the most common security techniques utilized are Endpoint Anti-Malware Software, Firewalls & Intrusion Prevention Systems; Conditional Access; Software Active Threat Analysis & Analytics (ATA); Role-Based Access Control; and Multi-Factor Authentication (MFA). The destruction of data varies similarly, depending upon the specific application in use, location of data, and the users responsible for maintaining that data.

The majority of data protection configuration and monitoring is handled in-house, by technology staff members and staff/administrators delegated to enforce retention schedules within their particular areas of expertise. However, in-house approaches frequently require the collaboration and support of third parties. Retention is also predominantly handled in-house and governed by the board-approved retention policy and the associated retention schedule. Enforcement of this retention policy may also involve collaboration with service providers, to ensure that data existing on cloud-based services is in fact permanently destroyed from these remote systems.

It is the district's legal obligation to ensure that the highest levels of security for this data are in place. Strong policies and plans are vital in data collection to safeguard privacy. Districts and schools must have a data protection infrastructure to ensure that personally identifiable student data is protected. Schools obtain guidance and training of student data safety from some resources such as Federal and State laws (FERPA), their district legal counsel, state professional organizations such as Intermediate Units, as well as other resources such as The National Institute of Standards and Technology, Multi State Information Sharing and Analysis Center, and Center for Internet Security.

Keeping current with data protections to ensure student privacy is a constant conversation and concern for districts – trying to find the balance between safeguarding privacy without hindering student learning, as well as the balancing act between "industry best practices" and the very real budgetary and personnel limitations of a school district.

We appreciate this Committee's interest in this important issue and welcome any questions you may have at this time. Thank you.