



Testimony of the Pennsylvania Association of Intermediate Units

Joint Hearing of the Senate Communications and Technology & Education Committees
on Student Data Privacy

Scott Major, CISSP, CISA, ITIL v3
Chief Information Officer, Berks County Intermediate Unit 14

October 18, 2022

Good morning Chairwoman Phillips-Hill, Chairman Martin, Chairman Kane, Chairwoman Williams and members of the Senate Communications and Technology and Senate Education Committees. My name is Scott Major. I am the Chief Information Officer of the Berks County Intermediate Unit (BCIU), and I am here this morning representing the Pennsylvania Association of Intermediate Units (PAIU). I want to thank you for the opportunity to testify on the critical issue of student data privacy as it pertains to Pennsylvania's 29 intermediate units (IUs) in their efforts to provide education and services to the 1.7 million children in Pennsylvania.

Berks County IU 14 is one of the 29 regional education service agencies in Pennsylvania. The system of intermediate units was created by the General Assembly in 1971 was originally designed to play a critical role in supporting public and private schools across the Commonwealth, as well as assisting the Pennsylvania Department of Education's (PDE) efforts to provide a thorough and efficient system of education. In the 51 years since then, intermediate units have transformed from a system that predominately served children with disabilities and provided instructional materials to schools to an ever-evolving, complex system that provides a broad range of services such as virtual learning opportunities, special education, early intervention services, technology infrastructure, workforce development programs, professional learning, transportation, curriculum development, joint purchasing, health care consortiums, human resource and business office support, alternative education, and a host of other programs and services.

Intermediate units have become so adept at creating programs and services, that today, some people erroneously identify intermediate units as private vendors, which of course we are not. Intermediate units are governmental agencies designed by the General Assembly to be a critical part of the education system, and to provide expertise and economies of scale on both the instructional and operational sides of schools.

As this evolution of intermediate units over time suggests, we house a plethora of sensitive student and family data corresponding to educational programming we provide and schools we serve. We also assist with the provision of technology services and resources to schools. Both the instructional and operational functions necessitate our prudent care in protecting this private information. Intermediate units work diligently to ensure that the data they receive, utilize and store is handled appropriately, confidentially and managed judiciously in the ever-evolving and interconnected world in which we live, learn and work.

For example, at my IU – Berks County Intermediate Unit – I have overseen the implementation of a formal cybersecurity program using the National Institute of Standards and Technology (NIST) 800-53 framework and the Center for Internet Security (CIS) controls. In addition, I have worked with several Berks County Districts and Bergen County schools in New Jersey in the implementation of their cybersecurity programs. I have conducted several workshops in the Berks County community on the security/privacy risks that impact children and their families.

We have worked to secure student data privacy by:

- Implementing Data Loss Protection (DLP) controls
- Encryption of data in transit and at rest
- Inventorying BCIU systems that house data, identifying the data types stored within those systems, and assigning risk
- Adoption of a zero-trust model
- Implementing a security education training & awareness program

Other BCIU related projects and considerations include:

- Electronic data archival and retention
- The expansion of BCIU's DLP controls
- Analyze and minimization of the use, collection, and retention of Personally Identifiable Information (PII)
- Conducting regular data privacy and protection assessments in alignment with NIST SP 800-122 (Protecting the Confidentiality of Personally Identifiable Information)

As you are aware, schools and intermediate units across the Commonwealth have vastly varying levels of resources available to them to meet their primary goal of educating students. Some intermediate units may have the resources to go beyond what we have done, and others simply do not, but still continue to prioritize the critical role in maintaining data privacy. In the absence of a statewide framework for student data privacy, and with necessary data reporting and information sharing with PDE, such as Pennsylvania Information Management System (PIMS), intermediate units and all schools grapple at the local level with the complexities of the management and security of our data and electronic systems that retain it. While intermediate units all strive to implement the utmost security and safety to protect our students, the absence of a statewide framework and correlating resources to implement a plan, we are left to figure out on our own how to ensure privacy is maintained and with what resources. This means that the many measures or sets of protocols put in place are as unique as each intermediate unit or school system implementing them. Intermediate units work at the regional level to place a structure around protecting sensitive data and to provide some supports, but see great value in having a statewide structure that identifies specific measures needed and milestones of success.

With the value that implementing a statewide framework could provide, we seek to continue our close partnership with the state and with PDE to assist in the process of building it. Intermediate units would be an excellent resource in the identification of expectations, best practices and recommendations for implementation of a framework, as well as provide insight into challenges in advance of any statutory changes.

Some examples of areas that warrant further discussion with intermediate units to determine next steps include:

- How and what data types will be shared between a school or intermediate unit and the Chief Data Privacy Officer, such as envisioned in Senate Bill 37?
- How to manage third party contractors that host student data (compliance requirements, standardized process for collecting and reporting)
- Intermediate Units often receive documents that contain PII from sources outside their normal operating environment (i.e. surveys community partnerships) that are not tied to a student record. How will IU's obtain assistance navigating sensitive topics related to the outlier types of data that schools may store? Are they reportable to the Chief Data Privacy Officer?
- Many IUs are using the NIST or CIS Framework to build their cybersecurity programs. Is there a framework on which the student data privacy and protection program based?
- What is the expectation of rate the of adoption for the compliance of schools and IU's? For example, annual milestones?
- Intermediate Units are often the liaison to the school districts when new or amended legislation is passed. Will there be training, tools and resources available for schools and IUs to help them implement their programs?

The conversation around student data privacy clearly involves many considerations and can become complicated very quickly. With intermediate units and individual schools having varying levels of expertise and resources to implement privacy protections, it is important also to include conversations around providing resources from the state to assure that recommendations can be properly implemented locally. Pennsylvania's school districts and intermediate units are subject to a large number of unfunded mandates, and we do our best to comply in ways that also assure sound stewardship of taxpayer dollars. At one time, intermediate units relied heavily on state budget appropriations for funding. However, today, intermediate units receive no direct funding from the legislature. Rather, we must rely upon entrepreneurial activities to meet the needs of the schools we serve. As such, we would strongly urge the state to couple any new requirements for protecting

student data privacy with appropriate funding and other resources to assist with effective implementation. Even activities such as compiling data, creating reports, implementing new systems or monitoring cyber activities take time and staff, and without additional dedicated funding, we would be forced to take resources away from other services to comply with new mandates, which would ultimately detract from achieving our educational mission.

Finally, it is worth noting that intermediate units have a wealth of technical expertise in the areas of broadband connectivity, online education, and even cybersecurity. We even manage our own statewide, high-speed, stable and secure educational network enabling collaboration between educators and students. PAIUnet connects the 29 intermediate units and their member school districts, as well as public library systems and charter schools, increasing connectivity to provide access to content and resources that are transforming how educational services are delivered. We played a key role in helping schools connect with their students remotely during the sudden closing of schools due to the COVID-19 pandemic. Intermediate units also provide expertise to the Pennsylvania Broadband Development Authority in their role to expand broadband connectivity statewide and distributing state and federal grant money for projects in unserved and underserved communities. I note these critical areas of technical involvement to show that not only are we connecting students with state-of-the-art technology for education, but we also stand ready to share our expertise and participate in solutions-oriented approaches to improving all aspects of education provision across the state.

Please feel free to reach out to me, my intermediate unit colleagues or PAIU staff as you explore the best next steps for protecting student data in Pennsylvania. We look forward to being a partner in assuring that student data is private and secure.

Thank you again for the opportunity to testify today and I would be happy to answer any questions.