Data Privacy

Protect the sensitivity of student data held within education data systems, while enabling the use of this data to inform education policy and practice.

What is the issue and why is it important? What if SREB states do not make adequate progress on this issue?

Schools and colleges collect enormous amounts of data for educational improvement through their student information systems, enterprise resource systems, learning management systems, library systems and vendor-managed systems – much of it is information that should remain private. The data held within these diverse systems, the enormous number of devices accessing these systems, and all the interactive technology tools constantly emerging for classroom use present both security and privacy concerns. Data security and privacy, though related, are different issues. Data security is about protecting technology systems against unauthorized access and maintaining the integrity of the data within those systems. Data privacy is about the confidentiality rights of the individuals involved, the types of data collected, and how it is used and shared.

The 1974 federal Family Educational Rights and Privacy Act (FERPA) provides parental access to education records and the opportunity to have those records amended. It also offers parents and some students control over the disclosure of information in student records. The Pupil Privacy Rights Act applies to the programs and activities of a state educational agency, local educational agency or other recipient of funds under any program funded by the U.S. Department of Education and goes beyond FERPA to regulate specific types of information gathered through surveys, analysis, or evaluation. More recent federal regulations address student data privacy and security, such as the Higher Education Opportunity Act amendments and the Every Student Succeeds Act. In addition to federal legislation, individual states have introduced hundreds of bills regarding student data privacy in recent years. The National Association of State Boards of Education (http://www.nasbe.org/wp-content/uploads/NASBE-Policy-Update-2015-Legislative-Session-Data-Privacy-June-2015.pdf) and the Data Quality Campaign have highlighted the data legislation in various states (http://www.nasbe.org/wp-content/uploads/2015-State-Legislation-6-9.pdf).

State and local education data governance policies should address five broad areas: transparency, privacy, collection, use and sharing. One data governance goal should be to ensure that data made public about students involves large enough samples in aggregate form to ensure that no information about individual students can be surmised. Only individuals holding positions that permit them to view sensitive data should have access, and these individuals are responsible for keeping data secure and available only to others with a legitimate need to review it. There must be clear policies about what data are collected, who is responsible for securing it, and who is involved in carrying out procedures. Compliance audits should be an integral part of data governance practices, and agencies should be subject to public pass/fail ratings on their compliance with these practices.

Compliance, however, follows training. Policies should be clear that everyone responsible for data privacy and governance must be properly trained, and whenever policies change, those involved in implementing the changes should be thoroughly briefed. Data are often entered by employees with the least amount of training about data use and risks. Schools and colleges need adequate funding to train users, secure data systems, provide technical support, and purchase sufficient data monitoring and security tools. Moreover, compliance must account for third-party systems that interact with an agency's own, to prevent unintended access or use of data and to protect user identity.

Schools and colleges need adequate funding to train users, secure data systems, provide technical support, and purchase sufficient data monitoring and security tools.

Balancing student data privacy with useful data analysis requires careful thinking. If legislation and policies are too restrictive, the data collected may not be useful in helping policymakers improve student outcomes. If they are too lax, students' privacy is put at risk. To prevent unintended consequences, policymakers should consult a diverse group (including teachers, instructional technology staff, data managers, principals/administrators, purchasing agents, and educational technology specialists) when reviewing proposed policies or legislation.