Guide to Key Considerations for Education Data and Information Technology Systems

Student Privacy & Data Security: A State Education Agency Discussion Framework

Question: What do CareFirst BlueCross BlueShield, Harvard University, the Army National Guard, and the Office of Personnel Management (OPM) have in common?

Answer: They all suffered a data breach in 2015.[i]

Background

In today's data and technology driven environment, a data breach is a continual risk. Because of data breaches at BlueCross BlueShield and OPM, as well as additional high profile incidents at Target and Sony, more parents, educators, and community members are raising questions about the security of data collected and used by a state education agency. The task for an agency is to manage and mitigate the risks and communicate effectively about the protections in place. The good news is, there is someone in your agency already focused on data privacy.

The Privacy & Security Workgroup of CCSSO's Education Information Management Advisory Consortium has developed the *Student Privacy & Data Security: A State Education Agency Discussion Framework* as a resource to assist chiefs and state education agency leadership in engaging in a robust and productive conversation within the agency. This guide should be used to support agency leadership in the use of data and technology in meeting your overall vision, mission, and goals.

Every state has defined and implemented policies to support the use of information to make key decisions while protecting individual privacy and maintaining the security of data. Maintaining individual privacy and data security is not as simple as a checklist, nor is it the job of one individual or office. Maintaining individual privacy and data security is an ongoing effort that requires work across a state education agency. It requires strong, consistent leadership to become part of agency culture.

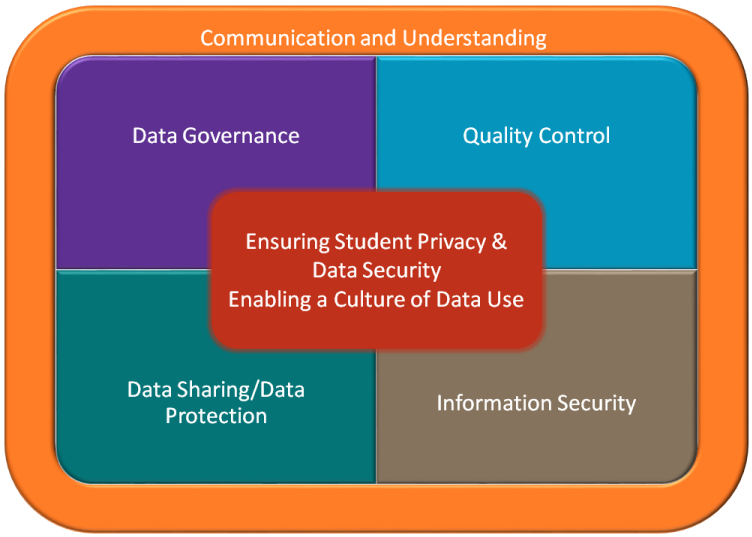
This new guide will help you support agency staff, communicate effectively about your agency's commitment to privacy and security, strengthen your agency's leadership in this area, and ensure your agency is well positioned to use information that supports your work.

How to Use this Resource

This document is intended to be used as a conversation starter between Chiefs and their Chief Information Officer, Chief Privacy Officer and education data and information systems teams

within the agency. The guide outlines questions to help agency leadership gain an understanding of their state's policy, practice, and implementation of privacy and security measures. This guide should be used as a starting point for deeper discussions on strengthening current practice and building a culture of data use within the agency.

The guide is organized into five sections - Communications and Understanding, Data Governance, Quality Control, Data Sharing/Data Protection, and Information Security. The sections will help you explore different areas of privacy and security policy implementation. Each section outlines key questions, provides a sample of evidence to look for in your state, and gives examples of effective practice.



It is important to remember that there is no one approach to quality implementation. States will each use different methods, structures, and engage different vendors. The most important factor in strong privacy and data security implementation is the support of agency leadership and a culture that values the need to secure all data within the agency's stewardship as well as the benefits offered by data-driven decision making.

We recommend that State Education Agency Chiefs use this document to engage staff in a conversation. This document will help you gain a better understanding of current agency practice and engage in a robust conversation on strengthening that work. It is intended to spark collaboration and discussion among agency leaders.

[i] At CareFirst BlueCross BlueShield 1.1 million records were compromised when hackers attacked the system in May. Harvard suffered a cyberattack in June exposing login credentials to access individual computers and university e-mail accounts. The July incident at the Army National Guard was the result of a mishandled data transfer to non-accredited data center by a contract employee which exposed the personally identifiable information of 850,000 current and form National Guard men and women. The breaches at the OPM were the biggest by far of 2015, first exposing the information of 4.2 million individuals in April, followed by the bigger hack of 21.5 million individual records in May. The slow and inadequate response to the hack resulted in the resignation of OPM director, Katherine Archuleta. (http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm)

Communication and Understanding

The use of education data is essential for the state education agency (SEA). Data allows us to make smart decisions on policy, resource allocation, and how to best support teaching and learning. We must ensure that the public understands why we collect data, how we use it, and what we do to protect it. The important question here is: ***Are we being proactive in providing the public with information about state education data collection, reporting, and use?***

Key Questions/Talking Points	Evidence	Effective Practice
Can various stakeholders across our state find and understand the information they need?	➢ Public reporting portal with easy-to-access and easy-to-understand data reports ➢ Links to SEA policies, to include high-level summary of data governance policies with explanation of what they mean to public (value of data sharing, how data is protected throughout process, etc.) ➢ A "one-stop shop" for privacy and governance information	The Colorado Department of Education has posted resources on their website, one click from the home page: • http://www.cde.state.co.us/dataprivacyandsecurity The Wisconsin Department of Public Instruction's WISEdash Public Portal allows districts, schools, parents, researchers, media and other community members to view data published by DPI. • http://dpi.wi.gov/wisedash South Dakota publishes a bi-monthly newsletter to communicate important information to districts. • STARS Connections – August 2015 Edition
What are we doing to help the public understand the need for data and data quality? Do we have a process for providing feedback or fielding questions from the public?	➢ Positive user stories ➢ Regular public meetings ➢ District champions to help communicate ➢ Strong website ➢ Dedicated inbox for comments/concerns	The Data Quality Campaign has great resources for demonstrating the value of education data and how it is used to support decision-making: • What is Student Data? • Mr. Maya's Data-Rich Year • Who Uses Student Data? • Ms. Bullen's Data-Rich Year
What policies, supports, outreach and/or training do we have in place to support local education agencies (LEAs), school systems, and schools in data governance?	➢ Link to policies in place to help LEAs, to include high-level summary of district guidance, set of policies that SEA follows to help districts ➢ Identification of training available with timelines ➢ State board and SEA policy statements and supporting organizational structures that bake this into normal operations	Alabama requires LEAs to have a locally adopted student records governance and use policy; the Alabama Department of Education provides support for the development of these policies: • Data Use and Governance in Alabama
The Key to Our Success: Communication and understanding is an important area for chief leadership in support of data use and privacy. Proper communication provides a platform to help stakeholders at all levels understand the importance of data use to support decision-making. Effective communications allow you to reinforce the efforts our agency undertakes to ensure privacy, confidentiality, and security.		

Data Governance

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures encompassing the full life cycle of data, from acquisition to use to disposal. The important questions here are: ***Do we have adequate policies/procedures/contracts in place to manage all internal and external data activities? Are we following all laws and state board directives?***

Key Questions/Talking Points	Evidence	Effective Practice
Do we share data with other state agencies? **If yes, what policies are in place to govern this data sharing?**	➢ Interagency data sharing processes ➢ Link to data sharing agreements and templates, identify governing bodies in place, e.g. cross-agency governance and data governance committees. ➢ Link to data request process, identify point person for incoming data requests, personally identifiable information (PII) vs. non-PII, etc.	Both the Washington Office of Superintendent of Public Instruction and the Wisconsin Department of Public Instruction have a detailed policy and process for requests of student-level data: • Data-Sharing Process and Policies for Student-Level Data (Washington) • WISE Data Requests (Wisconsin)
What are FERPA and COPPA and how do they apply to us? What other laws or regulations do we need to be concerned about?	Data Privacy and Security Alphabet Soup ➢ FERPA – Family Educational Rights and Privacy Act – protects the privacy of student education records ➢ COPPA – Children's Online Privacy Protection Act – establishes rules around the collection and use of personal information for children under 13 years of age ➢ FOIA – Freedom of Information Act – gives the right of citizens to access information from the government; regulations vary by state ➢ HIPAA – Health Insurance Portability and Accountability Act – protects the privacy of individual health information and can interplay with the student record in some circumstances including for students with disabilities and connections with child welfare	The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) is an incredible resource for information on implementing and ensuring compliance with these rules and regulations including: • FERPA 101 • Basic Concepts and Definitions • Data Governance Checklist • Protecting Student Privacy While Using Online Educational Services • FERPA/IDEA Crosswalk • Joint Guidance on the Application of FERPA and HIPAA to Student Health Records
Do we have clear data owners/stewards within our	➢ List of data owners ➢ Identification of gaps in data ownership list	Both the Kansas Department of Education and the Tennessee Department of Education have robust Data Governance

agency? Do those people understand their responsibilities? **What policies governing ownership and sharing do we have in place?** **What training do we provide for data owners/stewards?**	➢ Describe training provided and evidence the owners understand the associated accountability ➢ Data Governance Policy, Data Request Policies for PII and aggregated data ➢ Policies and procedures for data owners to approve release of data ➢ Policies and procedures to govern sharing and linking of data with other data sources, and risk assessments of resultant data sets	Programs including detailed descriptions of process, policies, and responsibilities. • Data Governance Program Handbook (Kansas) • Implementing Data Governance as the Foundation of a Longitudinal Data System (LDS) (Tennessee) The South Dakota Department of Education has developed a training program for their data coaches that includes navigating systems, using data to inform decisions, and roles and responsibilities: • SD-STARS Training Program • SD-STARS Implementation Planning Document • SD-STARS District Implementation Guide • South Dakota FERPA Website
The Key to Our Success: Leadership must emphasize the importance of data governance and change the culture within a state education agency to strengthen data privacy and security. As the head of a state education agency, leaders should understand the strategic importance of data governance and require agency-wide implementation.		

Quality Control

Accurate, timely, and quality data is essential to ensuring we have the information we need to make decisions, support our schools, and ensure transparency to our communities. The important question here is: ***How are we ensuring the public that the data we collect and use is accurate?***

Key Questions/Talking Points	Evidence	Effective Practice
What are we doing to help school systems and schools submit accurate and timely data? **What types of data checks/routines are we performing at the SEA on school systems and schools data?**	➢ Communications, professional development opportunities, certification of data managers, partnerships with professional organizations ➢ Agendas of professional development, meetings, online courses, webinars, etc. conducted by SEA and partnering organizations ➢ Summary of districts attending and not attending. Follow-up with districts not in attendance ➢ Link to data code manuals and other SEA guidance ➢ Procedures for adding business rules to data collections	The Georgia Department of Education provides ongoing training for districts on data collection and reporting to ensure quality of information. Georgia also provides useful information back to the district through the Georgia Tunnel. • New Coordinator Presentations and Webinars • Georgia's Data Conference • Georgia's Path to Personalized Learning The Alabama Department of Education provides annual spring and fall regional training for districts on data quality, student management system changes, and data submission timelines. • Alabama's Data Code Manual and Users Guide

	➢ Procedures for internal data checks/verifications	
What is our strategy for ensuring data sets maintain the privacy and confidentiality of individual students?	➢ Documentation and description, in Standard English, on website for public transparency as well as filtering and disclosure ➢ Procedures for management of cell size strategy in agency ➢ Understanding of cell size strategy, terms, and why they are important by leadership	The National Center for Education Statistics (NCES) published a technical brief that provides guidance for suppressing small cell sizes and maintaining privacy in aggregate reports: • Statistical Methods for Protecting PII in Aggregate Reporting The Maryland Department of Education has a process for controlling the aggregate data published to their website: • Maryland Statistical Process Control
What types of cross checks/validations are we performing on data business rules and calculations performed by our agency i.e. confirming that our priority school list is accurate?	➢ Procedures for internal data checks/verifications by data owners ➢ Routine procedures	The New York State Education Department has developed a process for allowing school districts the opportunity to verify data in the state repository. • Distributed Reporting Design Overview
The Key to Our Success: We collect high-quality, meaningful, consistent data to support improvements in education across our system. As the agency's leadership, you should stand behind the appropriate use of data to meet our goals.		

Data Sharing/Data Protection

Ensuring that we reach our state's education goals means that we seamlessly connect data across the P-20-Workforce pipeline. To ensure individuals meet their own educational goals, we need to provide access to data and the technology necessary to reach those goals. Data must be protected while supporting decision-making at all levels. The key question here is: ***How do we allow access to data while still ensuring the policies and procedures are in place to protect personally identifiable data?***

Key Questions/Talking Points	Evidence	Effective Practice
What types of agreements do we have in place, related to data sharing? What is our agency doing to ensure all contracts, grants, and memorandum of understanding (MOUs) have the needed clauses to protect privacy and confidentiality?	➢ Link to contracts, Interagency Data Sharing Agreements, Research Agreements ➢ Documented process for developing these agreements and all templates in use to create agreements	The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) has several resources around data sharing, including: • Protecting Student Privacy While Using Online Education Services: Model Terms of Service • Policies for Users of Student Data: A Checklist
Do we share PII with vendors? If so, what policies are in place to	➢ Standard contract language with privacy/security provisions	The Delaware Department of Technology and Information provides statewide resources and support for data security,

protect shared data? What about data reporting for grant purposes?	➢ List vendors currently sharing PII, awareness by the Chief of potential problematic vendors	management and cloud computing. Several resources exist including: • State of Delaware Cloud and Offsite Hosting Policy In 2014 the Future of Privacy Forum (FPF) and the Software & Information Industry Association (SIIA) announced a K-12 Student Privacy Pledge to safeguard student privacy built around a dozen commitments regarding the collection, maintenance, and use of student personal information. • http://studentprivacypledge.org/
What are our procedures in responding to data requests? How do they differ if request is for PII or not? **Do we treat educator data differently from student data? If so, how? What policies and procedures are in place?**	➢ Link to data request process ➢ Identification of point person for incoming data requests, institutional review board (IRB) vs. non-IRB, etc. ➢ Could be case-by-case basis, could all be treated the same, either way, verify with policy	Both the Missouri Department of Education and the Pennsylvania Department of Education have outlined procedures for responding to data requests for both student and teacher information. • Procedures for Protection of Individually Identifiable Information (Missouri) • Student Data Access and Use Policy (Pennsylvania)
The Key to Our Success: Appropriate access to data serves students, parents, teachers, schools, districts, our agency and the state in meeting our goals for student learning and success. Through strong leadership and solid management practice, we can support access to information while maintaining privacy and confidentiality of individuals.		

Information Security

Information security and physical premise safeguards are an important component in an overall data management strategy. Appropriate measures must be provided to ensure facility, hardware, and data security. Our premise and network security protocols and procedures are a key factor in managing physical and virtual access to facilities where educational data resides. The key questions here are: ***How do we ensure the data we collect is as secure as possible from potential breaches or misuse? How do we ensure the appropriate data protection is being applied at all levels?***

Key Questions/Talking Points	Evidence	Effective Practice
What policies, infrastructure and supports are in place to manage our data security?	➢ Policies such as SEA requirement to use consistent identity management tools ➢ Policies on data retention, data destruction, encryption in transit and at rest, cloud use and requirements, multi-level authentication	The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) has several resources around information security: • Data Security Checklist • Data Security: Top Threats to Data Protection

What gaps do we have (if any) in terms of information security controls that may need immediate attention?	➢ Review process for web posting of data ➢ Review processes for data requests and release, data sharing requirements ➢ Physical and procedural evidence of firewalls, filtering, anti-hacking infrastructure, security audits, server hardening reports ➢ Data security/IT procedure professional development for all staff ➢ Identification of the major gaps already known and what is needed to move forward to remedy the gap (e.g., encrypting databases at rest, need time and additional funding to accomplish this)	• Identity Authentication Best Practices Arkansas has articulated robust policies on all aspects of IT security and use best practice in implementation. • IT Security Policy • IT Best Practices
What is our retention and data destruction policy for student records? How do we verify destruction has occurred? **How well is this policy communicated to the public?**	➢ State, SEA, and local record retention policy and mapping from paper to electronic records ➢ Standard contract language with data destruction provisions ➢ Link to record retention policy on SDE website ➢ Training and support for LEAs on best practices	The U.S. Department of Education's Privacy Technical Assistance Center (PTAC) has a great resource for data destruction: • Best Practice for Data Destruction The Wisconsin Department of Public Instruction has created an online form to certify the destruction of data issued under a data use agreement: • DPI Certificate of Data Destruction
What are we doing to ensure all school, district, and state staff that have access to our applications have correct roles and permissions?	➢ Identification of tools in use for state access management along with accompanying policies defining how SEAs identify who has control of role definition at each district ➢ Identification of policies in place at SEA to oversee and support tool and process, etc.	The North Carolina Department of Public Instruction's Data Management Group sets policy around data access and roles. • Data Management Policies • Data Access Roles • DPI Access to Information and Systems Policy
The Key to Our Success: Mitigating a breach is more than just a technical exercise; leadership is essential in supporting and managing data security at all levels.		

Acknowledgements

This resource was developed by the Privacy & Security Workgroup of CCSSO's Education Information Management Advisory Consortium (EIMAC). CCSSO would like to thank the following CIOs for their leadership of this workgroup:

Marcia Bohannon, Chief Information Officer, Colorado Department of Education
Pat Bush, Chief Information Officer, Delaware Department of Education
Melinda Maddox, Deputy State Superintendent, Alabama Department of Education

Additionally, CCSSO would like to thank State Education Agency staff from the following states, from our Education Information Management Advisory Consortium members, who contributed greatly toward this work:

Alabama
Arizona
Arkansas
California
Colorado
Connecticut
Delaware
Department of Defense
Florida
Georgia
Hawaii
Idaho
Illinois
Kansas
Kentucky
Maine
Maryland
Massachusetts
Michigan
Mississippi
Missouri
Montana
Nebraska
Nevada
New Hampshire
New Jersey
North Carolina
North Dakota
Oklahoma
Oregon
Pennsylvania
South Carolina
South Dakota
Tennessee
Utah
Virginia
Washington
West Virginia
Wisconsin
Wyoming

The expertise and thoughtful feedback of the EIMAC Privacy & Security workgroup has been instrumental in the development of this resource.