DATA QUALITY CAMPAIGN
Using Data To Improve Student Achievement

Nelson Mullins
Nelson Mullins Riley & Scarborough LLP

EducationCounsel LLC

Complying with FERPA and Other Federal Privacy and Security Laws and Maximizing Appropriate Data Use

A STATE POLICYMAKERS' GUIDE

MARCH 2013

Executive Summary

State policymakers are tasked with balancing student privacy and supporting data collection and use, both of which are possible under the federal Family Educational Rights and Privacy Act (FERPA) and other federal student data privacy laws. State policymakers will not meet their goals of supporting effective data use and protecting the privacy, confidentiality, and security of student information without an understanding of these laws. If state policymakers are unable to distinguish between the laws' legitimate and perceived limitations and communicate with stakeholders about these issues, they will be unable to maximize use of data in support of their efforts to improve student achievement. For example, state policymakers may not realize that FERPA applies only to personally identifiable information and not aggregate data or that the law allows postsecondary student records to be shared with a student's former school district for evaluation purposes.

In addition to understanding and complying with FERPA, states also have the responsibility to understand and comply with state data privacy and security laws, as well as other federal privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) to the extent that data subject to those laws are incorporated in the state educational data system.

Finally, understanding federal privacy laws is only one step for state policymakers as they must not only understand privacy laws in their own states but also play a leadership role to ensure that the state is effectively protecting student information. **While state policymakers bear the responsibility for protecting student privacy, they need not do so at the sake of restricting the use of quality, longitudinal education data in support of their ultimate goal: improving student achievement.**

Policymakers' Responsibilities to Support Effective Data Use and Protect Student Information

State policymakers have the responsibilities to both protect student information and support effective data use to improve student achievement. When states collect the most relevant data and are able to match individual student records over time, they can answer questions that are at the core of educational effectiveness. Statewide longitudinal data systems are capable of providing timely, valid, and relevant data.

Using Appropriate Data to Improve Student Achievement

Appropriate access to statewide longitudinal data enables the following:

- ***Teachers** (as well as **parents**) have the information they need to tailor instruction and supports to help each student improve.*
- ***Administrators** have the resources and information to effectively and efficiently gauge progress and manage the execution of education strategies and programs.*
- ***Policymakers** are able to evaluate which policy initiatives show the best evidence of improving student achievement and preparing students for colleges and careers.*

Over the last decade, the state role in education has evolved to keep pace with the increased demand for timely and appropriate education data that are indispensable to policy, management, and instructional decisions. Empowering stakeholders—from parents and teachers to leaders and policymakers—with the high-quality data they need requires limited and appropriate sharing of data on students as they move through the education system and across traditionally siloed agencies and sectors.

There is also increasing demand to link limited and appropriate data on social services and early childhood care services, health data, and workforce data to meet important objectives. These objectives include, most critically, the ability to collaborate with others in meeting the needs of at-risk students and to measure the effectiveness of schools and school districts in preparing students for higher education and careers.

At the same time, use of data for these purposes needs to be harmonized with appropriate protections for the privacy and security of student records. This responsibility for state officials includes meeting the moral and legal obligations to respect and protect the privacy and confidentiality of students' personally identifiable information. It also includes mitigating risks related to the intentional and unintentional misuse of data, which are amplified by the digital nature of today's society in which more information—in education and every sector—is housed and shared in electronic and Web-based forms. It further requires clarity around roles and responsibilities, including states' authority to share data and the form in which the data can be shared as well as with whom the data can be shared and what protections need to be in place. *(See Appendix: Beyond FERPA—State Responsibilities and Critical Questions to Protect Student Data.)*

The Family Educational Rights and Privacy Act (FERPA)[1] imposes limits on the disclosure of student records[2] by educational agencies and institutions that receive funds from the U.S. Department of Education (ED). Many states have complementary laws on the privacy of student records,[3] and virtually all states have laws regarding data security that apply to education and other data.[4] In addition, links to data of noneducation agencies may implicate other laws on the privacy of data, including the Health Insurance Portability and Accountability Act (HIPAA).

FERPA at a Glance

FERPA's purpose and evolution will be discussed at length in the next section of this guide. However, key guidance regarding well-established FERPA interpretations includes the following:

- **Sharing student data that are not personally identifiable** is permissible. (See sidebar, right.)
- Even with regard to personally identifiable student information, clearly permissible disclosures (without written parent or eligible student consent) include the following:
  - **evaluating/auditing federal and state-supported programs and implementing school and district[5] accountability,** including disclosures of student data by postsecondary institutions to state educational agencies and school districts to evaluate how well they prepared students for college
  - **sharing state-level, as well as district-level, data with organizations to conduct research to improve instruction,** assuming state law expressly or implicitly gives the state this authority
  - **sharing student records with workforce and other noneducation agencies to evaluate** (or audit or ensure compliance of) **publicly funded education programs,** including any education programs administered by the workforce or noneducation agency
  - **monitoring and analyzing assessment, enrollment, and graduation data**
  - **sharing student records from a student's prior school with the student's new or prospective school**
  - **redisclosing data by the state education agency** for purposes and to recipients that come within **FERPA-authorized disclosures**
  - **maintaining a teacher identification system that links teachers and students** (and disclosing that information to the extent consistent with FERPA-authorized disclosures)

How FERPA Defines "Personally Identifiable Information"

FERPA specifically defines the term "personally identifiable information" as including, but not limited to, "[t]he student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier, such as the student's Social Security Number, student number, or biometric record; other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates." (34 CFR § 99.3)

In the 38 years since FERPA was enacted, the technology and culture around data collection and use have changed and so has the state role in collecting and using data, resulting in some uncertainty around how FERPA relates to state agencies and state longitudinal data systems. Over time, this uncertainty has been aggravated by the lack of relevant comprehensive—and consistent—federal guidance, particularly with respect to state data systems, and has had a chilling effect on the appropriate use of student records for important research, evaluation, and instructional needs. Many educators and policymakers are similarly uncertain about the application of other laws regarding the privacy and security of data as education data systems link to workforce, social services, health, and early childhood care data.

ED has begun to address this gap with the publication of amended FERPA regulations in December 2008 under U.S.

Secretary of Education Margaret Spellings;[6] the issuance of guidance in 2009 on the relationship between FERPA and HIPAA, issued jointly with the Department of Health and Human Services (HHS), under U.S. Secretary of Education Arne Duncan;[7] the publication of new FERPA regulations focused on state data issues on December 2, 2011;[8] the announcement of a new initiative to provide assistance and guidance to states on privacy and security issues;[9] and the creation of a series of best practice guides for state policies and practices for data systems.[10]

There is an immediate need for guidance as states build, refine, and use their state data systems. Recent federal law for the first time *mandates* use and certain disclosures of statewide data obtained from student records. For example, all states were required to sign assurances that they would establish state longitudinal data systems meeting all requirements of the America COMPETES Act as a condition of receiving funds under the State Fiscal Stabilization Fund (SFSF), authorized by the American Recovery and Reinvestment Act of 2009 (ARRA). Initially, states were required to establish these systems no later than September 30, 2011;[11] ED subsequently extended this deadline to January 31, 2012.[12] ED further extended the deadline for states to collect and publicly report data and information for SFSF requirements to December 31, 2012.[13]

Under implementing regulations for these laws, states are required to track specified data on the college enrollment and persistence of their former secondary school students who attend public institutions of higher education in their state and to link teacher and student data.[14] Similarly, to receive grants under the state longitudinal data system grant competition with funds provided under the ARRA, states are required to include postsecondary and workforce data in assisted data systems.[15] The practical imperative to provide guidance to states that harmonizes these obligations with their responsibilities to adhere to FERPA and other federal and state laws regarding the privacy and security of student records could not be clearer.

Federal Privacy Laws and Key Issues

This section provides an analysis of FERPA as it applies to state longitudinal data systems. It also analyzes the application of FERPA and other federal laws regarding the privacy of records to early childhood programs and provides a very brief discussion of other federal laws that may implicate the opportunity of state longitudinal data systems to obtain personal information from or share such information with workforce, public health, and other noneducation state and local agencies.

Student Education Records: FERPA

Background

In addition to giving parents rights to inspect and challenge the contents of their children's education records, FERPA generally prohibits educational agencies and institutions[16] from disclosing students' education records without written parent or eligible student consent.[17] "Student education records" are broadly defined to include any records, files, or documents that contain information directly related to a student and that are maintained by or for an educational agency or institution. However, FERPA limits on disclosure apply only to personally identifiable information on students. State longitudinal data systems generally may disclose aggregate, anonymous, and de-identified information derived from student education records. Further, if the data are personally identifiable, they still may be collected and disclosed without written parental consent

if the uses and recipients of the disclosure come within statutorily authorized disclosures (principally in FERPA itself). Several of these authorized disclosures relate to core functions of state longitudinal data systems.

Federal law does not provide a right for parents or students to sue in court for a FERPA violation.[18] The potential sanction for a FERPA violation is a cutoff of ED funds, but the law requires that ED seek voluntary compliance before imposing that remedy. Under prior regulations, that sanction applied only to educational agencies or institutions that enroll students, not to state education agencies, but the December 2, 2011, regulations extended that potential sanction to state education agencies. Also, the regulations clarify that state education agencies and districts or their authorized representatives for performing evaluation and audit functions are subject to debarment from receiving further student records from the educational agency or institution from which the records were obtained for a period of not less than five years, if they are determined by ED to have improperly redisclosed student records to others. These enforcement actions have rarely been threatened and have never been taken by ED since FERPA's enactment.

Permissible Data Sharing Under FERPA

Consistent with FERPA regulations and precedents of ED's Family Policy Compliance Office (FPCO), which administers FERPA, many data collection and disclosure practices relevant to state longitudinal data systems are clearly permissible under FERPA (without obtaining written parental or eligible student consent for each disclosure).

Sharing student data that are not personally identifiable is permissible. State longitudinal data systems may obtain and disclose anonymous or aggregate student information derived from student records provided the information is not personally identifiable.

Even in instances in which personally identifiable information on students is shared, clearly permissible disclosures (without written parent or eligible student consent) under FERPA include, but are not limited to, the following disclosures.

Evaluating/auditing state and local programs and implementing school and district accountability: States may create a data warehouse and use student data obtained from districts or public schools to evaluate the districts and schools and their programs and teachers, including making accountability determinations under federal and state laws. The 2008 FERPA regulations clarified that these functions could be performed by state education officials or by contractors to a state education agency, so long as the contractors do not redisclose personally identifiable information.

- **Disclosures to workforce and other noneducation agencies.** ED's December 2, 2011, FERPA regulations permit disclosures of student education records (without written parent or eligible student consent) to workforce and other noneducation state or local agencies for the purpose of evaluating (or auditing or ensuring compliance of) publicly funded education programs. An "authorized representative" of a state education agency or district (for purposes of receiving disclosures of student education records) is defined as any entity or individual designated by the state education agency or district to conduct an evaluation, audit, or compliance activity in connection with federal or state-supported education programs.

  The regulations do not, however, authorize disclosures of student education records to noneducation agencies for the purpose of evaluating or strengthening noneducation programs. That would require a statutory change.

  That said, the regulations may provide some flexibility on this issue by including a broad definition of education programs subject to FERPA's evaluation provision. The definition includes any program that is principally engaged in the provision of education, including job training, career and technical education, and early childhood education, irrespective of whether the program is administered by an education or noneducation agency.

In addition, as discussed below, the regulations authorize disclosures of education records to evaluate programs of the agency or institution receiving the records. Thus, the state education data system would be authorized to disclose student education records to a state workforce agency for the purpose of evaluating not only programs administered by state education agencies or districts but also job training programs administered by the workforce agency.

Under current law, these provisions appear to provide a reasonable and appropriately flexible solution for the management of student data by states. They would facilitate matching of data for the evaluation of education programs and appear to permit states to warehouse education records in centralized noneducation state data agencies under agreements with the state education agency to safeguard the data. These provisions appropriately are made subject to other provisions discussed on page 8 to ensure that the education records are properly used and safeguarded, including requiring reasonable methods to protect the records and agreements that limit their use and provide for their destruction when they are no longer needed for the evaluation.

With regard to disclosures for noneducation purposes, states may comply with FERPA by having the noneducation agency disclose its data to the state education agency or by matching the data between the two agencies under the supervision of the state education agency or through a contractor to the state education agency. The state education agency may then report nonpersonally identifiable information resulting from the match in aggregate form to the noneducation agency.[19]

» **Disclosures of postsecondary data to K–12 districts and of K–12 data to preschool programs.** As noted above, the December 2, 2011, FERPA regulations reinterpret FERPA provisions regarding the evaluation of publicly funded education programs to include such programs administered by any agency, not just the programs administered by the agency disclosing the student education records.

This reinterpretation means, for example, that disclosures of student records from a postsecondary data system or postsecondary institution to an elementary or secondary data system or agency would be authorized for the purpose of evaluating how well a K–12 district or school had prepared its former students for college. The regulation aligns ED's interpretation of FERPA with ED requirements under SFSF for specified data to be shared on postsecondary performance and persistence, reflecting on how well secondary schools prepared students for college.[20] The new interpretation also authorizes disclosing data on student performance in elementary schools to publicly funded early childhood learning and preschool programs: namely, to evaluate how well the early childhood learning and preschool programs prepared students for elementary school.

Conducting studies using state-level data to improve instruction: Aggregate or de-identified student information clearly may be disclosed to organizations for research purposes. In these instances FERPA simply is not implicated as FERPA does not apply to the disclosure of nonpersonally identifiable information.

The 2008 FERPA regulations indicate how personally identifiable information from student records may be de-identified for these purposes.[21] The FERPA statute also authorizes disclosure of personally identifiable information from student records without parent or eligible student consent for studies for or on behalf of educational agencies or institutions to improve instruction. The 2008 FERPA regulations implement this statutory provision by permitting educational agencies and institutions to enter agreements with research organizations to conduct studies using information disclosed from student records for that purpose. However, the 2008 FERPA regulations define "educational agencies or institutions" for purposes of this provision to exclude state agencies. As a result, state agencies in the past have been unable to disclose personally identifiable information from student records under this disclosure provision.

In its December 2, 2011, FERPA regulations, ED includes an interpretation that nothing in FERPA prevents a state education agency authority from entering agreements for studies to improve instruction on behalf of educational agencies or institutions in the state and to disclose education records to the research organization for that purpose. The provision for the first time applies the studies disclosure provision in FERPA to state-level data.

Monitoring and analyzing assessment, enrollment, and graduation data: Under the No Child Left Behind Act, states, districts, and schools may use data on state assessments, enrollment, and graduation not only to evaluate programs but also to track individual students and diagnose and address their specific needs and achievements.[22] This information can be shared with a school currently attended by each student. States may contract with other organizations to maintain and analyze these data.

Sharing student records among schools: Students' personally identifiable information may be passed on by students' prior schools or districts to current or prospective schools or districts. Sharing of this information is subject to notice to parents and the right of parents to contest the accuracy of the data.

Redisclosing data: Under the 2008 FERPA regulations, state education agencies may redisclose education records that they receive from a school or school district if the redisclosure is made to recipients and for purposes that come within any of the authorized disclosures in FERPA—for example, to a student's prospective school or to appropriate persons to protect the health or safety of the student or other persons in connection with an emergency. The state education agency must comply with FERPA requirements to maintain a record of such redisclosures—which may be maintained by the student's district, school, class, or other grouping (not necessarily by the name of each student) under the 2008 regulations—and must provide the record of redisclosure to the school or school district from which the education records were obtained, at its request.

Applying FERPA to Common Policy Scenarios

It is critical for policymakers to understand how FERPA applies to common scenarios related to high-priority efforts in their states. See below for common scenarios based on information drawn from regulations and ED's materials.

STATE LONGITUDINAL DATA SYSTEM	
Does FERPA permit schools and local education agencies, without parental consent, to provide students' education records to a state longitudinal data system?	Schools and local education agencies may disclose student records to a state education agency or other centralized state data entity, such as a statewide longitudinal data system, for purposes of evaluating (or auditing or ensuring compliance of) federal or state-supported education programs.
HIGH SCHOOL FEEDBACK REPORTS OR COLLEGE SUCCESS INDICATORS BY HIGH SCHOOL	
Does FERPA permit postsecondary entities or agencies to share student-level postsecondary data with the state education agency or districts for purposes of calculating postsecondary student enrollment and remediation rates by high school or school district?	The 2011 regulations allow such disclosures for purposes of evaluating how well districts and public schools prepared students for college.
SHARING DATA ACROSS STATE LINES	
May individual, student-level data be shared across state lines?	The preamble of the 2011 regulations states that nothing in FERPA specifically prohibits interstate disclosures that are made for the purposes of, and are consistent with the requirements of, the regulations.
RESEARCH STUDIES	
May a state provide student education records to an organization that proposes a research study to improve instruction?	The regulations clarify that nothing in FERPA bars the state from making these disclosures on behalf of districts or other educational institutions. The state should have express or implied authority under state law to do so and must enter an agreement with the research organization with safeguards prescribed in the FERPA regulations.

Maintaining a teacher identification system that links teachers and students: Neither FERPA nor any other federal law specifically addresses the privacy of information about teachers. However, information regarding which teacher is teaching which students generally may be disclosed only if disclosure is authorized under the other principles cited in this guide. For example, data linking public school teachers and their students could be disclosed to appropriate employees or contractors of a school district or the state data system for the purpose of evaluating publicly funded programs and teachers in those programs.

FERPA Safeguards and Enforcement

Particularly in its December 2, 2011, amendments, ED's regulations balance provisions for expanded access to student education records, as described above, with provisions to protect the privacy of student records and to enforce FERPA if these provisions are not adhered to.

Reasonable methods: The regulations require a state or local educational authority to use "reasonable methods" to ensure "to the greatest extent practicable" that any individual or entity designated as its authorized representative to receive data to conduct evaluations, audits, or compliance activities (1) uses student data only for authorized evaluation, audit, or other compliance purposes; (2) protects the data from further disclosure or other uses; and (3) destroys the data when no longer needed for the authorized purpose. ED has left flexibility to state and local educational authorities to determine those methods and has issued nonbinding guidance that accompanied its December 2, 2011, regulations with information on best practices in this area.

Written agreements: The regulations also require written agreements that address privacy safeguards between the state or local education authority and the authorized representative to which it provides data to carry out evaluations, audits, or compliance activities. The agreements, among other things, must designate the authorized representative; specify the information to be disclosed; describe the activity with sufficient specificity to make clear that it comes within an authorized purpose; provide for the destruction of the data when no longer needed for the authorized purpose (and specify the time period for such destruction); and establish policies and procedures to protect the student data from further disclosure and unauthorized use, including limiting use of the data to authorized representatives with legitimate interests in the purposes of disclosure.

Penalties for improper disclosure: The regulations require that if the FPCO finds that an authorized representative who receives personally identifiable information from education records to perform evaluations, audits, or compliance activities or any other third-party recipient of personally identifiable information from education records under FERPA improperly rediscloses the information in violation of FERPA, then the educational institution or agency from which the personally identifiable information originated would be required to deny the recipient further access to personally identifiable data for at least five years.

Additionally, state educational authorities and other recipients of funds under a program administered by ED—not just educational agencies and institutions that enroll students—are subject to investigations and enforcement, including possible withholding of funds, for FERPA violations. The regulations also require other third-party recipients of data to comply with reporting and informational requirements of ED in enforcing FERPA.

Complaints of violations: Finally, the regulations clarify that complaints of FERPA violations may be filed with FPCO by parents or eligible students; FPCO may investigate a possible violation in the absence of a complaint; and if FPCO finds a violation, it will give the noncompliant agency or institution an opportunity to come into voluntary compliance before taking any enforcement action, including actions to withhold funds and actions to debar a third-party agency or institution for at least five years from receiving further student data from the originating educational agency or institution.

Early Childhood and Preschool Education Records: FERPA and Other Federal Laws

The applicability of federal laws to the privacy of early childhood and preschool education records of children involves a complex patchwork that turns principally on the source of funding for agencies and institutions that conduct these programs. At the federal level, the principal sources of funds for preschool and early childhood education and care are HHS (through the Head Start Act and the Child Care and Development Block Grant Act of 1990) and ED (in particular, under Parts B and C of the Individuals with Disabilities Education Act and Title I of the Elementary and Secondary Education Act). Key elements of the early education patchwork include:

- If the agency that administers early learning and development programs is funded by ED, records on children receiving education services from that agency would be considered education records subject to FERPA, even if these services are funded by multiple programs. FERPA generally would apply to all student records maintained by the agency, not just the records of students served with ED funds.

- The scope of FERPA applicability, however, may remain somewhat unclear, even in cases of ED funding to early childhood programs. That lack of clarity is because FERPA applies to the education records of students. In many early childhood programs, it may be unclear whether all of the children are receiving education—with the effect that the children are deemed students for FERPA purposes—or noneducational child care. (If individual children are receiving a mix of education and noneducation child care services, ED likely would view their records as education records subject to FERPA.) ED may have resolved this issue in large part by including a broad definition of "early childhood education program" in its December 2, 2011, regulations to include, among other things, a state-licensed or regulated child care program. While it appears that this definition was included for purposes of defining the scope of FERPA-authorized disclosures to evaluate education programs, it seems unlikely that ED would seek to narrow that definition for purposes of FERPA applicability. Nevertheless, these issues have not been squarely addressed by ED.[23]

- For an agency administering a Head Start or an Early Head Start program, HHS is required by statute to issue regulations to ensure the confidentiality of personally identifiable data. The law provides that the regulations "shall provide the policies, protections, and rights equivalent to those provided to a parent, student, or educational agency or institution" under FERPA.[24] Proposed regulations to implement these provisions have yet to be issued. Pending issuance of the regulations, no federal privacy protections appear to apply to the records of children in Head Start programs unless the agency is also funded by ED.[25] State laws on the privacy of student records generally parallel or incorporate FERPA provisions. The answer may vary from state to state, but these laws likely would apply in most states to the records of children who participate in Head Start programs.

- The federal Child Care and Development Block Grant of 1990 includes no provisions that protect the privacy of records on children served under the program. These issues would generally turn on state law.

The net effect of this federal patchwork is that state data systems should generally have access to preschool, early education, and child care records for evaluation purposes, if consistent with relevant state law and so long as the administering agency does not have policies that prohibit or restrict that access. That is true whether the records are obtained directly from providers of these services or through elementary and secondary school systems that receive the records when the children matriculate to those schools. If child care records—or Head Start

or Early Head Start records, pending issuance of Head Start confidentiality regulations by HHS (for child care programs and Head Start agencies not funded by ED)—are obtained directly by the state data system, no federal laws constrain their use and disclosure by the state for legitimate educational purposes.

Another issue at both the state and local levels concerns disclosing a child's K–12 records back to the child's former preschool or early education or child care agency. If the child's former preschool or early education program is publicly funded and the purpose of sharing the child's records is to evaluate the program, the disclosure is authorized by FERPA, based on ED's interpretation in its December 2, 2011, regulations that the authority to disclose student records under the FERPA-authorized disclosure for evaluations is not limited to evaluations of programs administered by the disclosing agency. On the other hand, if the early childhood program is not engaged "principally in education," the education records could not be disclosed for the purpose of evaluating that program. Therefore, further clarification regarding the ability under federal law to share student records with early education providers is needed.

Workforce Data: FERPA and Other Federal Laws

Many educators have identified a significant need to match student education records with workforce data—in particular, confidential unemployment compensation information related to students or former students—to evaluate how well educational agencies, institutions, and programs prepared students for the world of work. ED has in the past taken the position that personally identifiable information from student records could not be disclosed to state or local workforce agencies, even if the purpose was to evaluate publicly funded education programs. To match the data in adherence with ED's view, it was necessary to disclose the workforce data to the education agency or institution, including the state educational agency or state longitudinal education data system. The education agency would perform the match and, as needed, disclose only aggregate information resulting from the match to the workforce agency. ED's December 2, 2011, regulations reverse this position and permit the state data system or state education agency to designate the state workforce agency as its authorized representative to match student and workforce records to evaluate publicly supported education programs.

In addition, the option remains to disclose confidential unemployment compensation data to the state education agency or data system for the purpose of matching the student and workforce data to evaluate education or workforce programs. Rules issued by the U.S. Department of Labor address minimum confidentiality and disclosure limitation requirements for unemployment compensation. Under these rules (Rule 603), confidential unemployment compensation information may be disclosed to a public official or to an agent or contractor of a public official for use in the performance of his or her official duties.[26] Thus, the disclosure of confidential unemployment compensation information to state education data systems is permissible under federal law. At the same time, states may adopt more restrictive rules than Rule 603, and many have done so. State education data systems need to carefully review their own state's rules for the use and disclosure of unemployment insurance information.

Health Information: FERPA and HIPAA

Difficult issues may arise if a state longitudinal data system wishes to link education and health data (for example, data maintained by state or local public health agencies). ED's traditional view has been that disclosures of education records to public health agencies are impermissible under FERPA, but the December 2, 2011, regulations reverse this position—if the purpose of the disclosures is to evaluate publicly funded education programs. If, by contrast, the plan is to disclose health information from the public health agency to the state education data system, the issue is whether such disclosure is permitted by HIPAA and what privacy and security restrictions would attach to such disclosures. If a state longitudinal data system seeks to link and obtain access to health information about students, it needs to address at the outset whether the information is covered by privacy and security requirements in HIPAA. Application of HIPAA may prevent acquisition of the information sought or subject the state data system to a detailed regulatory regime that was not designed for education data.

There is a common misperception that HIPAA applies to all health information, but that is not the case. HIPAA generally applies to "protected health information," defined to include information that could identify a person related to past, present, or future health condition or the provision of health care (likely, the kind of information that a state education data system would seek) but only for such information created or received by a "covered entity." "Covered entity" is defined to mean health plans (including state Medicaid and federal Medicare programs but not necessarily including state or federal health programs), health care providers that engage in payment and related transactions electronically, and clearinghouses for such transactions. It is also the case that HIPAA does not apply to health information that is subject to FERPA. That means if health information is maintained in school records—for example, in a school health office administered by an educational agency—its use and disclosure is governed by FERPA, not by HIPAA.

If HIPAA does apply, the information may be disclosed only if a HIPAA-compliant authorization is obtained from every individual (or a parent for a child who has not reached the age of majority under state law) whose information is to be disclosed or it comes within a limited list of excepted disclosures in HIPAA. The only excepted disclosure that may be generally applicable to disclosures to the state education data system relates to research, but only if the research and disclosures are approved by an institutional review board (generally useful only for medical research) or privacy boards established under HIPAA.

The state data system may be asked to sign an agreement designating the system as a HIPAA "business associate" but likely should avoid that status and agreement because business associates may generally use protected health information only for health-related purposes (treatment, payment, and health care operations). In addition, the Health Information Technology for Economic and Clinical Health Act[27] would subject state data systems signing such agreements to detailed HIPAA security requirements that were not designed for the maintenance and protection of education data.

Other Federal Privacy Laws

This section provides a brief overview of other federal laws that address the privacy and security of records along with a website link with additional background information.

Privacy Act of 1974: The Privacy Act of 1974 applies to systems of records with information on individuals maintained by federal agencies.[28] It does not generally apply to state and local government agencies. However, to the extent that a state data system seeks personal information maintained by a federal agency, such disclosures to the state would have to comply with the Privacy Act. For example, a state or local data system may have an interest in obtaining information on federal employees who were former students in its public education systems to determine how well they had prepared their students for the world of work, in much the same way that state and local data systems may seek unemployment insurance compensation records that help to address the same issue.

The Department of Labor has funded a pilot initiative—the Federal Employment Data Exchange System (FEDES)—that provides information on federal employees to participating states to help them meet their reporting requirements under federal and state laws and conduct performance measurements. About 40 states participate in FEDES. State workforce agencies are the primary state participants in FEDES, but a number of state education agencies also participate.[29]

Homeless Management Information Systems (HMIS): HMIS standards impose use, disclosure, and security requirements for protected personal information about a living homeless client or homeless individual.[30] The requirements apply to organizations that plan and coordinate services to the homeless. Under these standards, protected personal information may be disclosed for academic research pursuant to a written agreement. Such research would be subject to review by an institutional review board, which suggests that a state data system may need to partner with a research institution that has such a board to obtain this information.

Children's Online Privacy Protection Act of 1998 (COPPA): COPPA applies to websites operated for commercial purposes that collect information from children under age 13. COPPA generally does not apply to websites maintained by government agencies or nonprofit organizations. COPPA would apply to a state longitudinal data system only if the system collected information from children under age 13 on behalf of a commercial entity or commercial website. It does not apply where a school or public education agency has contracted with a website operator to collect information from children for the use and benefit of the school or public agency. If COPPA applies, the website operator needs to meet requirements in the law, including the posting of privacy policies and obtaining verifiable parent consent.

For further information on these federal laws, including more comprehensive summaries and additional resources, see supra note 4.

State Privacy/Security Laws and Issues

This section provides a brief analysis of state laws regarding the privacy and security of records. It includes a link to more complete information on the Data Quality Campaign's (DQC) website, including state-by-state summaries of laws regarding security and security breaches and use of Social Security numbers.

Privacy of student records: Many states incorporate FERPA privacy provisions regarding student records in their own state laws. Typically, state statutes or regulations incorporate the FERPA statute or FERPA regulations by reference. In other cases, state law establishes separate provisions regarding the privacy of student records, but those provisions closely track FERPA provisions.[31] State agencies that administer data systems need to review their own state laws regarding the privacy of student records, as well as cross-cutting state laws regarding data security, security breaches, and use of Social Security numbers, as summarized below.

State security measures: At least 28 states have laws that require the secure disposal or secure destruction of personal information or the implementation of security measures to protect such information. All of these laws apply to businesses, including private vendors of government agencies that maintain personal information, but some also expressly apply to government agencies. Almost all of these laws exempt encrypted information from their security requirements.[32]

Security breach notices: At least 46 states, the District of Columbia, and two territories have laws that require individuals to be notified in the event of a security breach of their personal information. The majority of these jurisdictions expressly apply these requirements to government agencies. Most of these laws apply only to electronic records; fewer than 10 states apply them to breaches of paper records. None of the state breach notification laws, with the exception of Wyoming's, require notification if the information is encrypted, and most exempt circumstances in which there is no reasonable or material risk of harm, identity theft, or fraud in connection with the compromised information. Several of these state laws require actions to prevent breaches.

Protecting Social Security numbers. At least 34 states have passed laws restricting the use and disclosure of Social Security numbers. Several of these laws apply to educational institutions and government agencies. Generally, the laws do not bar the use of Social Security numbers to link education and other data for purposes of evaluating publicly funded education programs or performing research to improve education. However, many of these laws prohibit educational agencies or institutions from using a Social Security number on student ID cards. Likewise, the December 2, 2011, FERPA regulations generally permit educational agencies and institutions to designate as directory information a student ID number on his or her ID card or badge but only if the ID number is not the student's Social Security number. (The federal Social Security Number Protection Act of 2010 also prohibits certain uses of Social Security numbers that are not generally relevant to state education data systems.)

Find Out More

For further information on state security, security breach, and use of Social Security number laws, including short summaries on a state-by-state basis, see "Using Data to Improve Education: A Legal Reference Guide to Protecting Student Privacy and Data Security" by DQC and Nelson Mullins Riley & Scarborough (www.DataQualityCampaign.org/resources/details/1246).

A Constantly Changing Landscape Will Require Ongoing Guidance

While ED's recent efforts have served to clarify significant issues about the application of FERPA to the current landscape, advances in technology and the increased demand for and supply of quality data continue to alter that landscape. There will always be new questions about how to *protect* student data. For example, as efforts move forward to provide parents and students with direct access to data, such as through the MyDataButton initiative, stakeholders are asking how this access will be limited to only that parent and student. And as more nongovernmental entities provide services to students, there are continuous questions about how those entities and schools, districts, and state educational agencies appropriately share and protect data.

State policymakers, education officials, parents, and other stakeholders will need ongoing clarity about how federal and state privacy laws apply to emerging roles and responsibilities; guidance on best practices for implementation, including those drawn from other economic sectors and industries; and tools for communicating this information effectively to stakeholders.

Conclusion

Policymakers play a significant leadership role in ensuring that effective use of data is balanced with appropriate protections of student data. When DQC launched in 2005, FERPA was the most often-cited barrier by states to collecting, sharing, and using data to improve student achievement. That problem should be ameliorated by ED's efforts to address the relationship of FERPA to state data needs, harmonize FERPA and the need to use student data for important educational needs, and provide more proactive technical assistance regarding data privacy and security issues. It is critical that policymakers understand FERPA to meet their legal obligations, navigate debates about appropriate collection and sharing, and communicate effectively with stakeholders regarding these issues.

Clarifying and enforcing FERPA is only one piece of the puzzle. Both DQC and ED have provided resources to help states meet their critical responsibility to implement strong policies and practices, aligned with best practices from other sectors, to protect student information.[33] As the data landscape continues to evolve to meet stakeholders' demands for data and keep pace with new technology, policymakers and educators at the local, community, state, and federal levels must work together to address these issues. Maximizing the effective use of data and protecting student information are not mutually exclusive goals.

Appendix: Beyond FERPA—State Responsibilities and Critical Questions to Protect Student Data

Through a ***common understanding of and commitment to privacy and security principles, addressing legal roadblocks*** preventing appropriate data use, and ***providing sensible implementation and oversight of strong policies and practices*** that protect student data from harm, the education sector can maximize investments in data systems, minimize data risks, improve data quality, and increase data management efficiency.

State policymakers have three overarching responsibilities to help protect the privacy, security, and confidentiality of students' personally identifiable information.

Establish roles for data stewardship: Define and clearly communicate authority, responsibility, and accountability for decisionmaking, management, and security of data.

Ensure policy documentation, transparency, and enforcement: Document laws, policies, and decisions related to data governance and communicate these policies and procedures in a way that is accessible to stakeholders, including agency staff, students, parents, and the public.

Support organizational capacity: Ensure the state has the capacity and resources to implement and sustain these policies and procedures, including staff and technical system infrastructure.

State officials responsible for the stewardship of student data and state data systems should ensure state policies and practices are designed to:

Justification	Justify that the student data being collected and stored are necessary, useful, accurate, and valid	» Have you established a discrete set of policy, programmatic, and operational needs that require the collection of student data? » Have you documented how data collections align with these needs and the source of the requirement? » Do you regularly review and update data collections to ensure only necessary data are collected? » Have you established policies and procedures for regularly and securely archiving or destroying student records? » Do you regularly audit data quality and accuracy processes?
Access	Limit access to personally identifiable information to necessary and appropriate individuals	» Have you defined multiple levels of access based on individuals' roles that limit the type of data individuals can access and for which students? » Do you take the necessary steps to restrict access to personally identifiable information and to de-identify such information? » Have you established internal procedural controls, including training and confidentiality agreements for staff who have access to data and mechanisms to track data access?
Sharing	Protect data that are shared from inappropriate use	» Have you established policies to guide decisions about whether to share data among state agencies, among postsecondary institutions, with researchers, and with third-party contractors? » When data are shared (including among state agencies, among postsecondary institutions, with researchers, and with third-party contractors), are sharing agreements put in place to ensure confidentiality? » When data are reported publicly in aggregate form, such as through state education agency websites or report cards, are the most robust methods used to protect personally identifiable information?
Security Framework	Implement a security framework that protects student information	» Have you developed a comprehensive security framework, including administrative, physical, and technical procedures for addressing information technology, project management, data, and security issues? » Do you implement training, monitor compliance, and regularly assess security operations? » Have you established policies and procedures for crisis management, including data losses and security breaches?
Proactive Communication	Provide public and parental notice about data collection, policies, access, and use	» Do you communicate with students, parents, and the public about what information is being collected and shared and why? » Do you annually notify students and parents about their rights under federal and state law, how they can access their student's information, and the processes to request changes to those data?

Endnotes

1. Section 444 of the General Education Provisions Act, 20 U.S.C. 1232g.
2. Throughout this document, references to "student education records" or "student records" refer to personally identifiable information in student records maintained by schools or local educational agencies. There is no FERPA issue with regard to the disclosure of information derived from student education records that is not personally identifiable.
3. See, e.g., Tex. Gov't Code Ann. § 552.001 (Texas); O.C.G.A. § 50-18-72(a)(1) (Georgia).
4. See Data Quality Campaign and Nelson Mullins Riley & Scarborough, "Using Data to Improve Education: A Legal Reference Guide to Protecting Student Privacy and Data Security" (2011), available at http://www.DataQualityCampaign.org/resources/details/1246.
5. For the purposes of this guidance, the term "district" is used to refer both to school districts and to local educational agencies that may not constitute school districts, such as charter schools.
6. 73 Fed. Reg. 74806 (December 9, 2008).
7. See U.S. Department of Education, "About the Family Policy Compliance Office," available at http://www2.ed.gov/policy/gen/guid/fpco/index.html.
8. 76 Fed. Reg. 75641 (December 2, 2011).
9. See Press Release, U.S. Department of Education, "U.S. Department of Education Launches Initiative to Safeguard Student Privacy," available at http://www.ed.gov/news/press-releases/us-education-department-launches-initiatives-safeguard-student-privacy.
10. See National Center for Education Statistics, "Data Systems Standards and Guidelines: Best Practices Guides," available at http://nces.ed.gov/dataguidelines/guides.asp.
11. Section 14005(d)(3) of the American Recovery and Reinvestment Act of 2009; 74 Fed. Reg. 58436, 58452-53 (November 12, 2009).
12. See Data Quality Campaign, "ED's Proposed Changes to SFSF Data Collection and Reporting Requirements—Initial Analysis" (September 23, 2011), available at http://www.DataQualityCampaign.org/files/SFSF Proposed Changes DQC Analysis.pdf.
13. 77 Fed. Reg. 4663 (January 31, 2012).
14. 74 Fed. Reg. at 58452, 58494-95; 58505.
15. Title VIII of the American Recovery and Reinvestment Act of 2009. Other federal programs mandate similar data connections and linkages. For example, the Workforce Data Quality Initiative requires linkage to K–12 data; the Race to the Top-Early Learning grant competition requires linkage to K–12 data; and the new state longitudinal data system grants have priorities for linkage to postsecondary, workforce, and early learning data.
16. FERPA regulations define "educational agencies and institutions" generally to be schools, postsecondary institutions, or local educational agencies that enroll students. 34 CFR 99.1. The new proposed FERPA regulations would extend that definition for purposes of ED enforcement remedies to any agency or institution that receives funds from ED, including state education agencies.
17. When a student turns 18 years old or is enrolled in a postsecondary institution, the right of a parent to consent to disclosure transfers to the student. The FERPA regulations use the term "eligible student" to refer to these students.
18. Gonzaga University v. Doe, 536 U.S. 273 (2002).
19. Congress enacted and the President signed into law on January 14, 2013, the Uninterrupted Scholars Act, Pub.L. 112-278. This law permits disclosure of student records to an agency caseworker or other representative of a state or local child welfare agency or tribal organization who has the right to access a student's case plan, as determined by the state or tribal organization, when such agency or organization is legally responsible, in accordance with state or tribal law, for the care and protection of the student. Such disclosures are subject to requirements that the education records not be further disclosed, except to an individual or entity engaged in addressing the student's education needs, as authorized by the agency or organization.
20. See supra note 14.
21. 73 Fed. Reg. at 74833-36 (December 9, 2008).
22. Sec. 1111(b)(3)(B) of the Elementary and Secondary Education Act, 20 U.S.C. 6311(b)(3)(B).
23. As a matter of public policy, privacy protections for the records of children in these programs should not turn on differentiating educational from child care services. The exact boundary between "education" and "care" is not easily defined at either a policy or practice level, and having important privacy protections reliant on that differentiation is unlikely to produce desirable outcomes.
24. Sec. 641A(b)(4) of the Head Start Act, as amended (42 U.S.C. 9836A(b)(4)).
25. HIPAA privacy regulations may apply in very limited instances to protected health information maintained by these agencies, as discussed in this guidance.
26. 20 C.F.R. Part 603; 71 Fed Reg. 56830.
27. 42 U.S.C. 1320d-5.
28. 5 U.S.C. § 552a.
29. See http://www.ubalt.edu/jfi/fedes/.
30. HMIS Standards Final Notice (2004), available at http://www.gpo.gov/fdsys/pkg/FR-2004-07-30/html/04-17097.htm.
31. See supra note 4.
32. Among notable state efforts, Nevada, for example, requires both businesses and government agencies to use encryption when externally transmitting personal information, and Massachusetts imposes much more extensive encryption requirements on personal information.
33. See http://www.dataqualitycampaign.org/build/legal_guide/federal_laws/family-educational-rights-and-privacy-act.

This guide was written by Lyndsay Pinkus and Alexandria Barkmeier of the Data Quality Campaign; Steve Winnick, Art Coleman, Scott Palmer, and Kate Lipper of EducationCounsel LLC; and Jon Neiditz of Nelson Mullins Riley & Scarborough LLP (with which EducationCounsel is affiliated). It updates 2007 and 2011 issue briefs prepared by the managing partners of the Data Quality Campaign based on previous legal analysis by Messrs. Winnick, Coleman, and Palmer. This issue brief is intended as information for educators and policymakers. It should not be construed as specific legal advice, and readers should not rely on the information contained within without legal counsel.

Nelson Mullins

Nelson Mullins Riley & Scarborough LLP

Nelson Mullins Riley & Scarborough LLP is a national law firm with a strong East Coast presence. It provides advice and counsel in litigation, corporate, economic development, securities, finance, intellectual property, government relations, and regulatory issues, including data privacy and security across multiple government and economic sectors.

EducationCounsel LLC

EducationCounsel LLC is affiliated with Nelson Mullins Riley & Scarborough. It is an innovative law, policy, strategy, and advocacy organization committed to strengthening education systems, closing achievement gaps, and expanding access to educational opportunities at all levels of education from birth and pre-school through elementary, secondary, and higher education. EducationCounsel collaborates with education leaders from across the country, including state and local leaders, higher education officials, associations, foundations, and pioneering private and public entities to improve educational outcomes for all students.

DATA QUALITY CAMPAIGN

Using Data To Improve Student Achievement

For more information visit www.DataQualityCampaign.org and follow us on Facebook and Twitter (@EdDataCampaign).

Click or scan the code for DQC's best tools and resources.

The **Data Quality Campaign (DQC)** is a nonprofit, nonpartisan, national advocacy organization committed to realizing an education system in which all stakeholders—from parents to policymakers—are empowered with high-quality data from the early childhood, K–12, postsecondary, and workforce systems. To achieve this vision, DQC supports state policymakers and other key leaders to promote effective data use to ensure students graduate from high school prepared for success in college and the workplace.

1250 H Street NW, Suite 825, Washington, DC 20005
Phone: 202.393.4DQC (4372) Fax: 202.393.3930 Email: info@dataqualitycampaign.org