



## ALIGNING THE EFFECTIVE USE OF STUDENT DATA WITH STUDENT PRIVACY AND SECURITY LAWS

*A Legal and Policy Guide for State Policymakers*

October 2011

---

This legal and policy guidance provides a summary framework for state policymakers as they work to use longitudinal data to improve student achievement while also protecting the privacy and security of individual student records.<sup>1</sup> Summarizing relevant federal privacy and security laws, with a focus on the Family Educational Records and Privacy Act (FERPA),<sup>2</sup> this guidance illustrates how constraints placed on states by federal privacy and security laws can be harmonized with the appropriate use of student data for significant educational purposes.

Key points of guidance regarding well-established FERPA interpretations, described below, include:

- Sharing student data that are not personally identifiable is permissible.
- Even with regard to personally identifiable student information, clearly permissible disclosures (without written parent or eligible student consent) include –
  - Evaluating/auditing state and local programs and implementing school and district<sup>3</sup> accountability.
  - Monitoring and analyzing assessment, enrollment, and graduation data.

---

<sup>1</sup> The guidance updates and expands guidance and suggestions provided by EducationCounsel and the Data Quality Campaign (DQC) in a March 2007 publication, *Maximizing the Power of Education Data While Ensuring Compliance with Federal Student Privacy Laws: A Guide for Policymakers*. This guidance does not provide specific legal advice, nor does it advocate any specific state or district action. Policymakers should consult with their legal counsel and the state attorney general's office, as appropriate, as they build, strengthen, and use their state longitudinal data systems.

<sup>2</sup> Notably, the U.S. Department of Education (USED) is expected to release final Family Educational Rights and Privacy Act regulations in early 2012. This guidance will be updated at that time to reflect any administrative changes.

<sup>3</sup> 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.

- Sharing student records from a student's prior school with the student's new or prospective school.
- Re-disclosing data 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).

In addition, key issues regarding unresolved FERPA interpretations (related to prospective final USED regulations based on April 8, 2011, proposed regulations) are analyzed, and include:

- Whether FERPA bars disclosures of students' education records without written parent or eligible student consent to workforce and other non-education state agencies.
- Whether a state education agency, data system, or educational institution's disclosure of student records for the purpose of evaluating federal- or state-supported education programs is limited to evaluations of programs of the disclosing agency, system, or institution.
- Whether student education records may be disclosed to a student's former school or school district.
- Whether a state longitudinal data system may disclose student education records to organizations to conduct research.

Finally, this guidance includes an overview of other relevant laws and key issues, including a discussion of federal laws that govern early education, workforce, and health information, along with suggested action steps policymakers should consider to ensure privacy and security while supporting the use of data.

## **I. BACKGROUND**

Educators and policymakers at all levels of government have come to recognize the need for better information, including state-level student information, as an essential tool for improving schools and raising student achievement. They understand that when states collect the most relevant data and are able to match individual student records over time, they can answer the questions that are at the core of educational effectiveness. To that end, policymakers, educators, and researchers need statewide longitudinal data systems capable of providing timely, valid, and relevant data. Appropriate access to these data:

- Gives teachers (as well as parents) the information they need to tailor instruction and supports to help each student improve,
- Gives administrators resources and information to effectively and efficiently gauge progress and manage the execution of education strategies and programs, and
- Enables policymakers to evaluate which policy initiatives show the best evidence of improving student achievement and preparing students for colleges and careers.

Educators and policymakers also have recognized the importance of linking certain data on social services and early childhood care services, health data, and workforce data to meet important objectives. These 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. In particular, FERPA<sup>4</sup> imposes limits on the disclosure of student records by educational agencies and institutions that receive funds from the U.S. Department of Education (USED).<sup>5</sup> Many states have complementary laws on the privacy of student records,<sup>6</sup> and virtually all the states have laws regarding data security that apply to education and other data.<sup>7</sup> In addition, links to data of non-education agencies may implicate other laws on the privacy of data, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Unemployment Insurance regulations, and the Privacy Act of 1974.<sup>8</sup>

In the 37 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. 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 also are similarly uncertain about the application of other laws regarding the privacy and security of data, as education data systems link to workforce, social service, health, and early childhood care data.

USED has aggressively begun to address this gap, with the publication of amended FERPA regulations in December 2008;<sup>9</sup> the issuance of guidance on the relationship between

---

<sup>4</sup> Section 444 of the General Education Provisions Act, 20 U.S.C. 1232g.

<sup>5</sup> Throughout this document, references to "student education records" or "student records" refer to personally identifiable information in student records maintained by schools or LEAs. There is no FERPA issue with regard to the disclosure of information derived from student education records that is not personally identifiable.

<sup>6</sup> See, e.g., Tex. Gov't Code Ann. § 552.001 (Texas); O.C.G.A. § 50-18-72(a)(1) (Georgia).

<sup>7</sup> 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>.

<sup>8</sup> See 42 U.S.C. § 300gg, 29 U.S.C. § 1181 *et seq.*, and 42 U.S.C. § 1320d *et seq.*; 20 CFR Part 603; 5 U.S.C. § 552a, respectively.

<sup>9</sup> 73 Fed. Reg. 74806 (December 9, 2008).

FERPA and HIPAA, issued jointly with the Department of Health and Human Services (HHS), in 2009;<sup>10</sup> the publication of new proposed FERPA regulations focused on state data issues on April 8, 2011;<sup>11</sup> the announcement of a new initiative to provide assistance and guidance to states on privacy and security issues;<sup>12</sup> and the creation of a series of best practice guides for state policies and practices for data systems.<sup>13</sup>

Although it is impossible to draw definitive conclusions based on the new proposed FERPA regulations until they are issued in final form, there is an immediate need for guidance as states build and refine 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;<sup>14</sup> USED recently extended this deadline to January 31, 2012.<sup>15</sup>) USED also recently proposed further extending the deadline for states to collect and publicly report data and information for SFSF requirements from September 30, 2011, to December 31, 2012.

Under implementing regulations for these laws, states are required to track specified data on 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.<sup>16</sup> Similarly, to receive grants under the state longitudinal data system (SLDS) grant competition with funds provided under the ARRA, states are required to include in assisted data systems postsecondary and workforce data.<sup>17</sup> The practical imperative to provide

---

<sup>10</sup> See U.S. Department of Education, "About the Family Policy Compliance Office," available at <http://www2.ed.gov/policy/gen/guid/fpc/index.html>.

<sup>11</sup> 76 Fed. Reg. 19726 (April 8, 2011)

<sup>12</sup> 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>.

<sup>13</sup> See National Center for Education Statistics, "Data Systems Standards and Guidelines: Best Practices Guides," available at <http://nces.ed.gov/dataguidelines/guides.asp>.

<sup>14</sup> Section 14005(d)(3) of the American Recovery and Reinvestment Act of 2009; 74 Fed. Reg. 58436, 58452-53 (November 12, 2009).

<sup>15</sup> See Data Quality Campaign, "ED's Proposed Changes to SFSF Data Collection and Reporting Requirements – Initial Analysis" (Sept. 23, 2011), available at <http://www.dataqualitycampaign.org/files/SFSF%20Proposed%20Changes%20DQC%20Analysis.pdf>.

<sup>16</sup> 74 Fed. Reg. at 58452, 58494-95; 58505.

<sup>17</sup> 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

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.

## II. 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 workforce, public health, and other non-education state and local agencies.

### A. Student Education Records: FERPA

#### 1. 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<sup>18</sup> from disclosing students' education records without written parent or eligible student consent.<sup>19</sup> 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 may disclose aggregate, anonymous, and de-identified information derived from student education records without regard to FERPA. 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.<sup>20</sup> The potential sanction for a FERPA violation is a cutoff of USED funds, but the

---

K-12 data; the Race to the Top-Early Learning grant competition requires linkage to K-12 data; and the new SLDS grants have priorities for linkage to postsecondary, workforce, and early learning data.

<sup>18</sup> 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 USED enforcement remedies to any agency or institution that receives funds from USED, including state education agencies.

<sup>19</sup> 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.

<sup>20</sup> *Gonzaga University v. Doe*, 536 U.S. 273 (2002).

law requires that USED seek voluntary compliance before imposing that remedy. Under current regulations, that sanction applies only to educational agencies or institutions that enroll students, not to state education agencies. However, the proposed regulations issued April 8, 2011, would extend that potential sanction to state education agencies. Also, the proposed regulations clarify that state or local education agencies 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 5 years, if they are determined by USED to have improperly re-disclosed student records to others. These enforcement actions have rarely been threatened and have never been taken by USED since FERPA's enactment.

## **2. Well-Established Permissible Data Sharing Under FERPA**

Consistent with FERPA regulations and precedents of the USED's Family Policy Compliance Office, 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:**

- **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 re-disclose personally identifiable information.
- **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.<sup>21</sup> This information can be shared with a school currently attended by

---

<sup>21</sup> Sec. 1111(b)(3)(B) of the Elementary and Secondary Education Act, 20 U.S.C. 6311(b)(3)(B).

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. This is subject to notice to parents and the right of parents to contest the accuracy of the data.
- **Re-disclosing data:** Under the 2008 FERPA regulations, state education agencies may re-disclose education records that they receive from a school or school district if the re-disclosure 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 re-disclosures – which may be maintained by the students' district, school, class, or other grouping (not necessarily by the name of each student) under the 2008 regulations – and must provide the record of re-disclosure to the school or school district from which the education records were obtained, at its request.
- **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, the link between 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.

### 3. Unresolved FERPA Issues and Evolving Interpretations

Several FERPA issues that implicate the needs of state longitudinal data systems have not been definitively resolved. These issues arise in part from the expanded role of the states and state longitudinal data systems in maintaining statewide data for research, evaluation, accountability, and (in some cases) instructional purposes for the benefit of schools and school districts throughout the state. They also arise in part from prior, discrete interpretations of FERPA by USED. Proposed regulations published on April 8, 2011, by USED address each of these issues. The key issues, how the proposed regulations would address these issues, and recommendations for USED or for the states regarding the issue are reflected below.

**Issue 1:** *Does FERPA bar disclosures of students' education records without written parent or eligible student consent to workforce and other non-education state agencies?*

Prior Regulations/Interpretations: Since 2003, USED's informal view has been that student records may not be disclosed to a non-education state agency, even for the limited purpose of evaluating or auditing education programs, because the state education agency does not control the other agency and the other agency therefore may not be deemed an "authorized representative" of the state education agency. Also, if the purpose of disclosures to a workforce or other non-education state agency is to evaluate or strengthen the non-education programs administered by that agency, the FERPA statute does not permit these disclosures of personally identifiable information from student records. Such disclosures do not generally fit under any of the authorized disclosures in the law.

Proposed Regulations/Recommendations: USED's new proposed regulations would reverse its prior interpretation with regard to disclosures made for the purpose of evaluating or auditing publicly funded education programs. They define an "authorized representative" of a state or local education agency to mean any entity or individual designated by the state or local education agency to conduct an evaluation, audit, or compliance activity in connection with federal or state-supported education programs.

The proposed regulations do not, however, authorize disclosures of student education records to non-education agencies for the purpose of evaluating or strengthening non-education programs. That would require a statutory change. That said, the proposed regulations may provide some flexibility on this issue by proposing a broad definition of education programs subject to FERPA's evaluation provision. The proposed 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 non-education agency. In addition, as discussed under Issue 2, the proposed regulations would authorize disclosures of education records under the FERPA evaluation provision to evaluate programs of the agency or institution receiving the records. Thus, the state education data system would be authorized under these proposed provisions to disclose student education records to a state workforce agency not only for the purpose of evaluating programs administered by state or local education agencies, but also for the purpose of evaluating job training programs administered by the workforce agency.

Under current law, these proposed provisions would 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 would appear to permit states to warehouse education records in centralized non-education state data agencies under agreements with the state education agency to safeguard the data. They are appropriately made subject to other proposed provisions 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 or return when no longer needed for the evaluation.

With regard to disclosures for non-education purposes, states may comply with FERPA by having the non-education 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 non-personally identifiable information resulting from the match in aggregate form to the non-education agency.

**Issue 2:** *Is the authority of a state or local education agency, data system, or educational institution to disclose student records for evaluation of federal- or state-supported education programs limited to evaluations of programs of the disclosing agency, system, or institution?*

Prior Regulations/Interpretations. In the preamble to its 2008 FERPA regulations, USED expressed the view that disclosures under FERPA provisions authorizing disclosures for audits or evaluations of federal- or state-supported education programs are limited to audits or evaluations of programs of the disclosing agency or institution.<sup>22</sup> This would mean, 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 only if the purpose of the evaluation is to evaluate postsecondary programs. That interpretation would exclude what is presumably the principal purpose of sharing postsecondary data with an elementary or secondary data system or agency; namely, to evaluate how well elementary and secondary schools prepared the student for college. The interpretation likewise excludes the likely central purpose of disclosing data on student performance in elementary schools to publicly funded early childhood learning and pre-school programs: namely, to evaluate how well the early childhood learning and pre-school programs prepared students for elementary school. This position also undermines USED requirements under the State Fiscal Stabilization Fund for specified data to be shared on postsecondary performance and persistence reflecting on how well secondary schools prepared students for college.<sup>23</sup>

Proposed Regulations/Recommendations: In its new proposed FERPA regulations, USED would reverse its prior position, interpreting the authority to disclose student records for evaluation to encompass *any* evaluation of federal or state-supported education programs, consistent with the language of the FERPA statute. This proposed change would resolve the issue.

**Issue 3:** *May student education records be disclosed to a student's former school or school district?*

Prior Regulations/Interpretations. FERPA authorizes disclosures of student records to a school in which a student newly enrolls or intends to enroll. It does not include an express authorization to disclose student records to a school or school district in which a student previously was enrolled. In the preamble to its 2008 FERPA regulations, USED expressed the view that such disclosures are not generally authorized.<sup>24</sup> However, as discussed under

---

<sup>22</sup> 73 Fed. Reg. 74822, 74829 (December 9, 2008).

<sup>23</sup> See *supra* note 14.

<sup>24</sup> 73 Fed. Reg. 74829 (December 9, 2008).

issue 2, FERPA authorizes disclosures of student records to state or local officials for the purpose of evaluating federal or state-supported education programs. Disclosures to a student's former public school district for evaluation purposes would appear to come within the language of the statute.

Proposed Regulations/Recommendations: This issue is parallel to Issue 2. The proposed regulations would reverse USED's prior position by interpreting the authority to disclose records to local education officials for evaluation to include disclosures to local education agencies for the purpose of evaluating elementary and secondary programs, consistent with the language of the FERPA statute. The proposed change would also authorize education records to be provided by elementary and secondary schools and agencies to providers of publicly funded preschool and early childhood education programs for the purpose of evaluating those programs. The proposed change would resolve these issues.

**Issue 4:** *May state longitudinal data systems disclose student education records to organizations to conduct research?*

Prior Regulations/Interpretations: It is clear that aggregate or de-identified information 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 non-personally identifiable information. The 2008 FERPA regulations indicate how personally identifiable information from student records may be de-identified for research purposes.<sup>25</sup> 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, and the 2008 FERPA regulations implement this statutory provision by permitting educational agencies and institutions to enter agreements with research organizations to conduct these studies using information disclosed from student records for that purpose. However, current FERPA regulations define "educational agencies or institutions" for purposes of this provision to exclude state agencies. As a result, state agencies have been unable to disclose personally identifiable information from student records under this disclosure provision.

Proposed Regulations/Recommendations: In its proposed FERPA regulations, USED includes an interpretation that nothing in FERPA denies a state education agency authority to enter agreements for research 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 proposed provision would for the first time apply the research studies disclosure provision in FERPA to state-level data.

---

<sup>25</sup> *Id.* at 74833-36.

## **B. Early Childhood and Pre-school Education Records: FERPA and Other Federal Laws**

The applicability of federal laws to the privacy of early childhood and pre-school 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 pre-school 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 USED (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 USED, 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 USED funds.
- The scope of FERPA applicability, however, may remain unclear, even in cases of USED funding to early childhood programs. That 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 non-educational child care. (If individual children are receiving a mix of education and non-education child care services, it is likely that USED would view their records as education records subject to FERPA.) These issues have not been squarely addressed by USED and may require legislation to resolve.<sup>26</sup>
- For an agency administering a Head Start or 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.<sup>27</sup> Proposed regulations to implement these provisions are expected to be issued in 2011 or thereafter. Pending issuance of the regulations, it appears that no federal privacy protections apply to the records of children in Head Start programs unless the agency is also

---

<sup>26</sup> 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.

<sup>27</sup> Sec. 641A(b)(4) of the Head Start Act, as amended (42 U.S.C. 9836A(b)(4)).

funded by USED.<sup>28</sup> 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 Childhood 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 at the state level of this patchwork is that state data systems should generally have access to pre-school, early education, and childcare 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 Head Start agencies not funded by USED) – are obtained directly by the state data system, there are no federal laws that constrain their use and disclosure by the state for legitimate educational purposes.

A harder issue at both the state and local levels concerns disclosing a child's K-12 records back to the child's former pre-school or early education or child care agency. If the child's former pre-school or early education program is publicly funded and the purpose of sharing the child's records is to evaluate the program, the disclosure should be authorized by FERPA, provided that USED adopts in final regulations its position in the new proposed FERPA 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 to share student records with early education providers under federal law is needed.

### **C. 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 – in order to evaluate how well educational agencies, institutions, and programs prepared students for the world of work. As noted above, USED 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 USED's view, it was necessary to disclose the workforce data to the

---

<sup>28</sup> HIPAA privacy regulations may apply in very limited instances to protected health information maintained by these agencies, as discussed in this guidance.

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. USED's April 8, 2011, proposed regulations would 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 in order 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 in order to evaluate education 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.<sup>29</sup> 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.<sup>30</sup>

#### **D. 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). USED's traditional view has been that disclosures of education records to public health agencies are impermissible under FERPA, but the April 8, 2011, proposed regulations would 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 the Health Insurance Portability and Accountability Act (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

---

<sup>29</sup> 20 C.F.R. Part 603; 71 Fed Reg. 56830.

<sup>30</sup> For further information, *see supra* note 7.

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 only use protected health information for health-related purposes (treatment, payment, and health care operations). In addition, the HITECH Act<sup>31</sup> 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.<sup>32</sup>

### **E. 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.

**1. Privacy Act of 1974** – The Privacy Act of 1974 applies to systems of records with information on individuals maintained by federal agencies.<sup>33</sup> 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 their public education systems in order 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

---

<sup>31</sup> 42 U.S.C. 1320d-5.

<sup>32</sup> For further information, *see supra* note 7.

<sup>33</sup> 5 U.S.C. § 552a.

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.<sup>34</sup>

**2. 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.<sup>35</sup> 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 in order to obtain this information.<sup>36</sup>

**3. COPPA** – The Children's Online Privacy Protection Act of 1998 (COPPA) applies to websites operated for commercial purposes that collect information from children under the age of 13. COPPA generally does not apply to websites maintained by government agencies or non-profit organizations. COPPA would apply to a state longitudinal data system only if the system collected information from children under the age of 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 applied, the website operator would need 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 7.

### III. 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 website, including state by state summaries of laws regarding security and security breaches and use of social security numbers.

- **Privacy of Student Records.** Many state laws incorporate FERPA privacy provisions regarding student records in their own state laws. Typically, state

<sup>34</sup> See <http://www2.ubalt.edu/jfi/fedes/index2.cfm>.

<sup>35</sup> *HMIS Standards Final Notice* (2004), available at [www.ich.gov/library/fr-hmis.pdf](http://www.ich.gov/library/fr-hmis.pdf).

<sup>36</sup> For further information, *see supra* note 25.

statutes or regulations incorporate the FERPA statute or FERPA regulations by reference.<sup>37</sup> In other cases, state law establishes separate provisions regarding the privacy of student records, but those provisions closely track FERPA provisions. 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.<sup>38</sup>
- **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 new proposed 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.)

---

<sup>37</sup> See *supra* note 6.

<sup>38</sup> 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.



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 <http://www.dataqualitycampaign.org/resources/details/1246> (Data Quality Campaign and Nelson Mullins Riley & Scarborough, "Using Data to Improve Education: A Legal Reference Guide to Protecting Student Privacy and Data Security").

#### **IV. State Policymaker Actions To Ensure Privacy and Security while Supporting the Use of Data**

This section discusses a number of recommended actions that state education leaders, working with their legal counsel in the state agency and the state attorney general's office, should consider, as needed and appropriate, as they continue to build, strengthen, and use their state longitudinal data systems.<sup>39</sup> State policymakers should consider these steps and frame their own state-specific plan of action to align their state longitudinal data system with privacy and security protection laws.

##### Review and Possible Revision of State Laws, Policies and Practices

1. Review the final FERPA regulations that will be adopted in the coming months. The proposed regulations can be viewed at <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.
2. Review state privacy and security laws to ensure that the state longitudinal data system complies with state law. DQC's website, at [http://dataqualitycampaign.org/build/legal\\_guide/](http://dataqualitycampaign.org/build/legal_guide/), provides a catalog of state privacy laws and guidance/checklists regarding privacy, security, and confidentiality and education data for state policymakers to consider.
3. Review and clarify state law, regulations, and guidelines –
  - To authorize the state longitudinal data system to redisclose education records for FERPA-authorized purposes and recipients, including research studies for the benefit of school and education agencies in the state.
  - If the state maintains separate P-12 and postsecondary data systems, to authorize each system to receive records from the other system and/or from individual schools or school districts for purposes of evaluating, auditing, or ensuring compliance with the requirements of state and federal education programs and to make it clear that the

---

<sup>39</sup> See Data Quality Campaign, *Supporting Data Use While Protecting the Privacy, Security and Confidentiality of Student Information: A Primer for State Policymakers* (July 2011), available at <http://www.dataqualitycampaign.org/files/DQC-Privacy-primer%20Aug24%20low%20res.pdf>.

evaluation authority encompasses evaluations of programs at all levels of education.

4. Through state regulations and guidelines or through appropriate agreements with schools and school districts, allocate responsibilities for implementing FERPA procedures (e.g., parent notices, records of disclosures, rights to contest content of records) and clarify these responsibilities for parents.
5. Promulgate through state statute or regulations a definition of education programs for the purpose of determining which programs are subject to the evaluation provisions in FERPA, including programs in areas such as early childhood services and job training.
6. Develop procedures to respond to security breaches, consistent with state law.

#### Data Governance Policies and Agreements

1. Review and revise as appropriate data governance policies that clearly address roles and responsibilities for protecting privacy and security; stakeholder input into the system; interoperability with the data systems of individual schools and local agencies and with the data systems of other state agencies; and programs to train users on how to use the system effectively and on their responsibilities to protect the data from unauthorized use or disclosure.
2. Develop agreements that address privacy safeguards, including those mandated by FERPA, between:
  - Postsecondary institutions and the agencies that manage the longitudinal data system to match records for purposes of evaluating the performance of LEAs and elementary and secondary schools in preparing students for college.
  - The longitudinal data system and workforce agencies, public health agencies, and social service agencies that provide or match data on clients to the longitudinal data system, or that receive data from the longitudinal data system as its authorized representative to conduct evaluation of publicly-funded education programs.
  - The longitudinal data system and its contractors involved in the maintenance or analysis of student education records.
3. Revise or develop proper data governance policies and administrative and electronic processes to ensure proper use and access to data only by

authorized users/recipients. Perfection is not the standard, but the policies and procedures need to be reasonable in light of the state of the art and what other sectors are doing.

### Transparency

1. Take steps to ensure schools and school districts inform parents (in their annual FERPA notice to parents) of the role of the state longitudinal data system in maintaining records, of the categories of state longitudinal data officials who will have access to the records, and of the allocation of responsibilities for implementing FERPA procedures and rights.
2. Develop and disseminate transparent policies on the broad purposes for which the state longitudinal data system uses student education records, the types of officials/contractors who have access to the records, and how the records are protected from unauthorized disclosures.

### **V. Conclusion**

Federal law authorizes and supports state longitudinal data systems, which are intended to facilitate more robust and effective use of data for improving education and meeting the academic needs of students, consistent with core state and federal policy and law. Through state longitudinal data systems, states, educators, and researchers can access and use student data to meet these purposes without violating privacy rights that federal law also protects. States need to give careful attention to federal and state legal requirements regarding the privacy and security of student records as they carry out these purposes. FERPA and other federal and state laws discussed in this paper impose important privacy and security constraints. Those constraints can and must be harmonized with the need to use student records for significant educational purposes as a foundation for evidence-based education reform and improvement.

*This guide was written by 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 a 2007 issue brief 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.*