CHILDREN'S EDUCATIONAL RECORDS AND PRIVACY

A STUDY OF ELEMENTARY AND SECONDARY SCHOOL STATE REPORTING SYSTEMS

October 28, 2009

FORDHAM
LAW SCHOOL

CENTER on
LAW and
INFORMATION
POLICY

Joel R. Reidenberg
Professor of Law and
Founding Academic Director
Jamela Debelak, Esq.
Executive Director

Student Project Fellows (Research & Drafting):
Adam Gross
Lee Mayberry
Judith Simms
Elizabeth Woodard

Student Project Fellows (Research):
Camilla Abder
Luke Bagley
Lisa Cooms
Ezra Kover

ACKNOWLEDGEMENTS

This study was prepared as a research project of the Fordham Center on Law and Information Policy (CLIP) in connection with the educational mission of the Fordham University School of Law. Under the supervision of Professor Joel R. Reidenberg, Jamela Debelak, as the Leitner Fellow and subsequently as the Executive Director of CLIP, led the team of Fordham students in their research and preliminary drafting of this study. Joel Reidenberg and Jamela Debelak did the final editing of the report.

Funding for this project was provided by CLIP and CLIP gratefully acknowledges the financial support of the Fordham alumni and benefactors whose generosity makes the Center's activities, programs, and research possible.

The views and opinions expressed herein are not presented as those of Fordham University, the Fordham University School of Law nor any of the financial supporters of CLIP.

FORDHAM CENTER ON LAW AND INFORMATION POLICY

CHILDREN'S EDUCATIONAL RECORDS AND PRIVACY:
A STUDY OF ELEMENTARY AND SECONDARY SCHOOL STATE REPORTING SYSTEMS

EXECUTIVE SUMMARY

Among state departments of education there has been a growing trend to establish statewide longitudinal databases of all K-12 children within a state in order to track students' progress and change over time. This trend is accompanied by a movement to create uniform data collection systems so that each state's student data systems are interoperable with one another. These two trends raised privacy concerns that we examine in this study. First, we were concerned with the way states were ensuring the privacy of their K-12 students. Specifically, our goal was to investigate what type of data was being collected and whether children were protected legally and technically from data misuse, improper data release, and data breaches. Second, we were concerned with the ease with which individual interoperable state data systems could potentially be combined to create a national database of all K-12 children.

We reviewed publicly available information from all 50 states and found that privacy protections for the longitudinal databases were lacking in the majority of states. We found that most states collected information in excess of what is needed for the reporting requirements of the No Child Left Behind Act and what appeared needed to evaluate overall school progress. The majority of longitudinal databases that we examined held detailed information about each child in what appeared to be non-anonymous student records. Typically, the information collected included directory, demographic, disciplinary, academic, health, and family information. Some striking examples are that at least 32% of the states warehouse children's social security numbers, at least 22% of the states record children's pregnancies, at least 46% of the states track mental health, illness, and jail sentences as part of the children's educational records, and almost all states with known programs collect family wealth indicators.

We found that, given the detailed and sensitive nature of the information collected, the databases generally had weak privacy protections. Often the flow of information from the local educational agency to the state department of education was not in compliance with the privacy requirements of the Family Educational Rights and Privacy Act. One state, New Jersey, even diverts special education medicaid funding to pay for an out-of-state contractor to warehouse data, including medical test results. Many states do not have clear access and use rules regarding the longitudinal database and over 80% of the states apparently fail to have data retention policies and are thus likely to hold student information indefinitely. Several states, like Montana, outsource the data warehouse without any protections for privacy in the vendor contract.

From our review, we were able to formulate several critical recommendations that we believe will increase the privacy, transparency, and accountability of these longitudinal databases:

1) Data at the state level should be anonymized through the use of dual database architectures;

2) Third party processors of educational records should have comprehensive agreements that explicitly address privacy obligations;

3) The collection of information by the state should be minimized and specifically tied to an articulated audit or evaluation purpose;

4) Clear data retention policies should be instituted and made mandatory;

5) Access and permissible use policies should be well articulated and specific in nature;

6) Audit logs of access to and use of the state databases should be maintained as a guard against unauthorized data processing;

7) Information about the database, its security, and its use should be readily available and verifiable.

8) States should have a Chief Privacy Officer in the department of education who assures that privacy protections are implemented for any educational record database and who publicly reports privacy impact assessments for database programs, proposals, and vendor contracts.

TABLE OF CONTENTS

I. INTRODUCTION

Since the passage of the *No Child Left Behind Act of 2001*,[1] ("NCLB") there has been an increase in data collection by educational agencies at the K-12 level. The reporting requirements of the NCLB and a general interest in individualizing instruction have generated a desire to gather information and track student progress over time. In furtherance of these goals, a trend has developed among state departments of education to create unified statewide longitudinal databases of student information. These databases typically store information about all K-12 children within the state's public schools at the state level over an extended period of time.

The desired benefits of these longitudinal databases have been well articulated by their proponents. First, some level of data collection at the state level is necessary in order for states to comply with the reporting requirements of NCLB. In addition however, individualized information collection can be used by teachers and administrators to evaluate both specific teaching methods and generalized trends among various schools in order to effect change that is designed to improve student progress.

The goal of this project was to examine the privacy protections afforded to these longitudinal databases. The study focused on basic privacy principles that are raised by state collections of children's information:

1) Control of personal information and data minimization: we examined the level of individual control over information. We considered whether states were requiring collection of excessive amounts of information and whether parents had an adequate ability to withhold private information;

2) Permissible uses of collected information: we looked for restrictions on the permissible use of the children's information. Fair information practice principles require a legitimate and appropriate use of all information collected and a mechanism to identify and correct misuse. Appropriate uses should protect children from public exposure and data manipulation; and

3) Data security: we looked at the security of the system holding the information in order to ensure that states were properly protecting personal information from errant access, disclosure and misuse.

Privacy protection is a significant concern, because whenever personal information is amassed in electronic format, there is a risk of data breach and data misuse. This concern is heightened when the information collected is sensitive and when the targeted group is a vulnerable population, such as school-age children. Past misuse of information regarding children illustrates this concern. For example, in 2003, the Student Marketing Group and American Student List, two information brokers that sold data pertaining to youth populations, were investigated by the Federal Trade Commission and the Office of the NY Attorney General for their data collection and data use practices.[2] The practices that were challenged by these law enforcement agencies included collecting information without parental consent from surveys administered in classrooms and then selling the compiled data to telemarketers.[3]

[1] Pub. L. 107-110. 115 Stat. 1425 (Jan 8, 2002).

[2] *See* David Koeppel, *Holding the Reins in Marketing to Youth*, N.Y. TIMES, Feb. 17, 2002, at 14LI; Warren Strugatch, *Marketing Company to Destroy Files*, N.Y. TIMES, Feb. 2, 2003, at 14LI .

[3] *See* People v. Student Marketing Group, Consent Order and Judgment #403543/02, NY Sup. Ct. Part 6 (2003), *available at* http://epic.org/privacy/student/SMGconsentorder.pdf

This study, thus, examines the longitudinal databases in place to determine whether there are appropriate mechanisms to protect the privacy of K-12 children and, if not, to recommend changes that would better ensure the security and fair use of children's educational records. The study seeks to identify the types of personal information that are being collected at the state level in order to evaluate the level of sensitivity of the data. The study reviews the regulations and technological measures in place to protect the privacy and confidentiality of the information held at the state level. By examining both the types of information collected and the privacy protections attached to the databases, the study seeks to highlight potential security and misuse problems while many of these systems are still in the development phase so that changes can be implemented before privacy harms become inevitable. Our findings are summarized below.

First, we found that data collection at the state level is often in excess of what is required by the *NCLB* and in excess of the data actually needed to evaluate overall school progress. The majority of longitudinal databases that we examined hold detailed information about each child, often in a non-anonymous student record. In general, there appears to be little distinction between the type of information that is held at the local level and the type of information that is passed onto the state departments of education. The information collected in the state databases includes demographic information, detailed disciplinary information, health information, academic information, and family information.[4]

Second, we found that, given the detailed and sensitive nature of the information collected, the databases generally have weak privacy protections. In most cases, the flow of information from the local educational agency to the state department of education does not appear to comply with the privacy requirements of the Family Educational Rights and Privacy Act.[5] In addition, many states do not have clear access and use rules regarding the longitudinal database and appear to hold student information indefinitely.

Finally, in our review of the 50 states, we found a few states that had clearly thought about privacy concerns and had implemented some effective protections. From these states, we formulated a series of best practices for privacy protection. We present these recommendations at the end of this report.

These recommendations are critical because the privacy of the nation's children is currently at significant risk from the existing databases. Without greater attention to privacy, information about children's elementary, middle and high school experiences and behavior is an open book. The vulnerability of these data trails to hacking and to misuse jeopardize children today and leave them exposed as adults to be haunted by the incidents of their childhood.

[4] *See infra* apps. A-G.

[5] 20 U.S.C. § 1232g (2005).

II. BACKGROUND

A. Methodology

We began by doing a survey of each of the 50 states to determine which states had or were developing student longitudinal databases. Our initial research team collected publicly available information from the websites of the state departments of education during the spring and summer of 2008.[6] The information collected included data dictionaries, user manuals, summaries of the data systems, privacy and security guidelines, press releases, and public presentations. When we were unable to find sufficient information online regarding the data elements that were collected by a particular state or regarding the way the information system operated, we followed up with a phone call to those specific state departments of education. From the calls we were usually either able to obtain additional documentation about the system, or we learned that the database was still in the development stages and additional information was not yet available.[7]

If the information we collected mentioned that the state used a third party vendor for the development of the system or for the storage of the data, we also made a request for a copy of the agreement with such third party vendor. Most states responded promptly; however, as of the date of this report, we have not received requested contracts from a few of the states.[8] Also, some states may use third party vendors without disclosing those relationships publicly on their websites.

The information on each of the states' programs is current as of November 1, 2008, when we concluded the primary research phase of this study. Because of the nature of the programs and their development, it is unlikely that substantive changes have occurred since our research cut-off date.

Once the information was collected, the second research team reviewed all of the documents and categorized the information into several tables.[9] We created three tables focused on (i) the data elements collected, (ii) the privacy protections applicable to the database, and (iii) the creation of and future plans for the database, respectively. These tables appear in Appendices A through G.[10] The second research team then analyzed the tables to identify trends.

B. Statutory Framework

Data collection regarding K-12 students is governed at the federal level by two statutes. First, the *Family Educational Rights and Privacy Act*, or "FERPA," was enacted in 1974 and provides certain minimal privacy protections for educational records.[11] Second, *No Child Left Behind Act*, or "NCLB," was promulgated in 2002[12] and established reporting requirements that initiated a need to increase data collection at the state level. The requirements of these two statutes and their impact on state longitudinal databases are discussed below.

[6] The initial research team consisted of Camilla Abder (FLS '08), Luke Bagley (FLS '09), Lisa Cooms (FLS '08), and Ezra Kover (FLS '08).

[7] We did not receive additional information from the following states: Alabama, Arkansas, Idaho, Maryland, Nevada, Oklahoma, Utah, Washington, and West Virginia.

[8] We did not receive vendor contracts or responses from Ohio and Rhode Island.

[9] The second research team consisted of Adam Gross (FLS '10), Lee Mayberry (FLS '10), Judith Simms (FLS '10), and Elizabeth Woodard (FLS '09).

[10] The tables reproduced in the Appendices are the consolidated results.

[11] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2005).

[12] No Child Left Behind Act of 2001, 20 U.S.C. §§ 6301-7916 (2002).

1. FERPA

FERPA was passed to protect the privacy of student educational records by regulating to whom and under what circumstances records may be disclosed. FERPA applies to educational agencies and institutions that receive federal funds administered by the Secretary of Education.[13] Under FERPA, an educational agency or institution is "any public or private agency or institution which is the recipient of funds"[14] if the institution "provides educational services or instruction, or both, to students" or if the institution "is authorized to direct and control public elementary or secondary…educational institutions."[15] The Family Policy Compliance Office ("FPCO")[16] has stated in advisory letters that, based on this definition, most local public schools and school districts, or local educational agencies, are subject to FERPA.[17] The office has also provided that, "[w]hile a [state educational agency ("SEA")] may receive funds from the [U.S. Department of Education], as a practical matter, FERPA generally would not apply to the records of an SEA . . . since students generally are not in attendance at an SEA."[18] However, FERPA's requirements regarding disclosure would apply to a state educational agency when that agency receives student educational records from a school district or local educational agency.[19] FERPA's requirements and prohibitions therefore apply to the individual schools that receive federal funding and provide educational services, to the school districts or local educational agencies that receive federal funds and direct such schools, and to states when they receive educational records as permitted under the statute. The only remedy for a violation of FERPA is the withholding by the U.S Department of Education of all federal funding.[20] Our research could not find any instance of the Department of Education withholding federal funds for a FERPA violation.

a. Educational Records

FERPA defines educational records to include information "directly related to a student" and "maintained by an educational agency or institution or by a party acting for such agency or institution."[21] Records include student files, student system databases kept in storage devices, or recordings and/or broadcasts.[22] The records regarding each student that are generated by the local schools are educational records under FERPA and therefore disclosures by the local schools for inclusion in a statewide longitudinal database must meet FERPA's requirements. Educational records are comprised of two types of information, directory information and non-directory information, and these two components have different disclosure protections under FERPA.

[13] Family Educational Rights and Privacy Act Regulations, 34 C.F.R. § 99.1 (2000).

[14] 20 U.S.C. § 1232g(a)(4).

[15] 34 C.F.R. § 99.1.

[16] FPCO was established by the Secretary of Education after the passage of FERPA. FPCO is charged with "investigat[ing], process[ing], and review[ing] complaints and violations under the Act . . . and provid[ing] technical assistance to ensure compliance with the Act." In this capacity, FPCO provides advisory letters to school and educational agencies regarding statutory interpretation. *See, e.g.*, 20 U.S.C. § 1232g(g); 34 C.F.R. §§ 99.60 – 99.67.

[17] *See* Advisory Letter from FPCO to the California Department of Education (Feb. 18, 2004) [hereinafter California 2004 FPCO letter] (on file with CLIP); Advisory Letter from FPCO to the Pennsylvania Department of Education (Feb. 25, 2004) [hereinafter Pennsylvania 2004 FPCO letter] (on file with CLIP).

[18] California 2004 FPCO letter, *supra* note 17; Pennsylvania 2004 FPCO letter, *supra* note 17.

[19] 20 U.S.C. § 1232g(b).

[20] 20 U.S.C. § 1232g. The Supreme Court has held that there is no private right of action under FERPA. Gonzaga Univ. v. Doe, 536 U.S. 273 (2002)

[21] 34 C.F.R. § 99 Subpart A (2000).

[22] 20 U.S.C. § 1232g(a)(4)(A).

Directory information may include any of the following: "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student."[23] Educational institutions are required to notify parents regarding what information from the above list they have defined as directory information.[24] Schools may typically disclose directory information without written consent from parents, however, a parent can choose to restrict the release of directory information by submitting a formal request to the school to limit disclosure.[25] Disclosure of directory information therefore operates under an opt-out system. Educational institutions are free to publicly disclose this information unless a parent submits a request to opt-out of disclosure.

Educational records may also consist of non-directory information. Non-directory information is all other information related to a student and maintained by an educational agency or institution including, without limitation, social security numbers, student identification numbers, race, ethnicity, gender, and transcript or grade reports.[26] Subject to certain exceptions discussed below, prior written consent is required before institutions can disclose non-directory information. Prior written consent must include the following elements:

(i) specification of the records to be disclosed;
(ii) the purpose of the disclosure;
(iii) identification of the party or class of parties to whom the disclosure is to be made;
(iv) date;
(v) signature of the parent of the student whose record is to be disclosed; and
(vi) signature of the custodian of the educational record.[27]

In addition, educational faculty and staff can only access non-directory information if they have a legitimate academic interest to do so.[28]

As we will discuss below in further detail, non-directory information that contains personally identifiable information or that is tied to personally identifiable directory information receives heightened disclosure protections under FERPA. According to the regulations implementing FERPA, personally identifiable information is any "information that would make the student's identity easily traceable," including: the student's name, the name of the student's parent or other family member, a personal identifier, such as a social security number or student ID number, or a list of personal characteristics that would make the student's identity easily traceable.[29] FPCO has advised that "data that cannot be linked to a student by those reviewing and analyzing the data" will not be deemed "personally identifiable."[30] The office has provided the following additional guidance regarding how agencies and institutions can create such

[23] *Id.* § 1232g(a)(5)(A).

[24] *Id.* § 1232g(a)(5)(B).

[25] *Id*.

[26] *See*, *e.g.*, 34 C.F.R. § 99.3 (2008); Will R. Van Dusen, Jr., NATIONAL ACADEMIC ADVISING ASSOCIATION CLEARINGHOUSE OF ACADEMIC ADVISING RESOURCES, FERPA—Overview, http://www.nacada.ksu.edu/Resources/FERPA-Overview.htm (last visited Mar. 18, 2009) (providing basic FERPA guidelines for faculty and staff).

[27] 20 U.S.C. § 1232g(b)(2).

[28] *Id.* § 1232g(b)(1)(A).

[29] 34 C.F.R. § 99.3.

[30] Advisory Letter from FPCO to the Tennessee Department of Education (Nov. 18, 2004) (on file with CLIP).

anonymous records using non-personal identifiers to ensure that records will not be deemed personally identifiable:

> "a student is identified **only** by a non-personal identifier **and** the following requirements are met:
>
> 1. the non-personal identifier itself –
>   a. is not a scrambled social security number or student number, unless such identifiers are protected by written agreements reflecting generally accepted confidentiality standards within the research community; and
>   b. cannot be linked to an individual student by anyone who does not have access to the linking key;
> 2. the anonymous data file is populated by data from educational records in a manner that ensures that the identity of any student cannot be determined, including assurances of sufficient cell and subgroup sizes; **and**
> 3. the linking key that connects the non-personal identifier to the student information is itself an education record subject to the privacy protections of FERPA. In other words, the linking key must be kept within the agency or institution and must not be shared with the requesting entity."[31]

For this report, the above guidance suggests that if an educational agency or institution creates a non-personal identifier for each record, but does not allow the receiving entity access to the database that generated such identifiers, the records disclosed might not be considered personally identifiable. Such interpretation relies, however, on an assumption that the information and characteristics disclosed, taken together, do not allow identification of a specific student. So, for example, if a non-personal identifier is used to release a record indicating that an anonymous ethnic minority male student with a disability at a specified elementary school had a certain score on standardized tests, and that elementary school has only one ethnic minority male in its students-with-disabilities program, such record would still be identifiable to that student and contain personally identifiable information. Therefore, the record would be subject to the heightened disclosure protections discussed below. In order to avoid this problem, agencies and institutions must use statistical methods to ensure that smaller demographic groups are not reported in such a fashion.[32] If however, a local educational institution is able to anonymize the data, then disclosure of the non-directory information would be permissible under FERPA without parental consent.

b. Rights Afforded Under FERPA

FERPA provides parents of K-12 students with the following rights regarding educational records:

- the right to inspect and review their child's education records;[33]
- the right to seek to amend information in the records they believe to be inaccurate, misleading, or an invasion of privacy;[34]
- the right to annual notification of information concerning their rights;[35] and

[31] *Id.*

[32] *Id.*

[33] 20 U.S.C. § 1232g(a)(1).

[34] *Id.* § 1232g(a)(2).

[35] *Id.* § 1232g(e).

- the right to consent prior to the disclosure of non-directory and personally identifiable information in their child's education records.[36]

When a student turns 18 years old or enters a post-secondary institution, these rights transfer from the parents to the student.[37] Educational agencies and institutions receiving federal funding must comply with each of these rights with respect to the information they forward to the state department of education for inclusion in a statewide student database.

Parents also have the right to inspect and review their child's educational records maintained by the school.[38] Schools are not required to provide copies of the records to parents unless it is impossible for parents or eligible students to review the records onsite. When copies are needed, schools may charge a fee for such copies.[39]

Parents who obtain access to educational records pursuant to FERPA and find information that they consider inaccurate, misleading, or a violation of privacy, may initiate a request to amend those records.[40] If the educational agency or institution involved declines to make the requested amendments, then they must afford the students or parents an opportunity for a hearing to challenge the content of the records. This hearing must be conducted within a reasonable time of the parent's request and on reasonable advance notice to the parents. The decision of the agency or institution must be based solely on the evidence presented at the hearing. If the records are not found to be inaccurate, misleading, or in violation of the student's rights, the parents have the right to place a statement in the records commenting on the contested information or stating why they disagree with the decision of the agency or institution.[41]

A school must annually notify parents of their rights under FERPA.[42] The notice must inform parents that they may inspect and review their children's education records, seek amendment of inaccurate or misleading information in their children's educational records, and consent to most disclosures of personally identifiable information from the educational records. The annual notice must provide information about how to file a complaint of an alleged violation with FPCO. It also must include a description of who is considered to be a school official, a definition of a legitimate educational interest, and information about who to contact to seek access to or amendment of educational records. Means of notification can include local or student newspaper, calendars, student programs guide, rules handbook, or other means likely to inform parents.[43]

Finally, prior written consent is generally required before institutions can disclose non-directory, personally identifiable information.[44] This general restriction applies any time a school or district agency discloses non-directory, personally identifiable information outside of such school or agency. Disclosures to state departments of education or third party vendors are therefore prohibited unless they meet the requirements of one of the exceptions discussed below. It is important to note for purposes of this report, that information which is disclosed only with a student ID number, rather than a student name, is still personally identifiable under FERPA and subject to this heightened protection. Only when an agency or institution removes all personally

[36] *Id*. § 1232g(b).

[37] 34 C.F.R § 99.5 (2000). The educational institution may, however, disclose the student's educational records to his/her parents if the student is the parents' tax dependent. 20 U.S.C. § 1232g(b)(1)(H); 34 C.F.R. § 99.31(a)(8)

[38] 20 U.S.C. § 1232g(a)(1).

[39] 34 C.F.R. § 99.11.

[40] 20 U.S.C. § 1232g(a)(2).

[41] 34 C.F.R. §§ 99.21-99.22.

[42] 20 U.S.C. § 1232g(e).

[43] U.S. Department of Education, FERPA for Parents, http://www.ed.gov/policy/gen/guid/fpco/ferpa/parents.html (last visited Feb. 26, 2009).

[44] 20 U.S.C. § 1232g(b).

identifiable information and assigns the records non-personal identifiers in compliance with the FPCO guidance above, are disclosures to outside parties permitted without prior consent.

c. *Exceptions to the Right to Consent to Disclosure of Educational Records*

FERPA's general rule requiring written consent of the parent for disclosure of non-directory information in educational records has several exceptions. First, as we discussed above, educational records may be released without consent if all personally identifiable information has been removed.[45] Additional exceptions, discussed in turn below, include: (i) disclosure to school officials with legitimate educational interests; (ii) the transfer of a transcript when a student changes schools or applies for admission elsewhere; (iii) disclosures in connection with studies undertaken on behalf of the school when such research can be conducted confidentially and anonymously; (iv) disclosures in connection with audits conducted by federal or state officials; and (v) disclosures in connection with records kept by law enforcement units.[46]

FERPA allows an educational agency or institution to disclose educational records without prior written consent to school officials within the agency or institution who have legitimate educational interests.[47] Generally, if a school official is performing an official task for the educational institution that requires access to information in educational records, that official is deemed to have a legitimate educational interest.[48] Under this exception, a third party may be considered a school official if such party is operating under the authorization of the institution and is performing an educational task that a school official would usually perform.[49] In a 2004 letter to a parent, the FPCO stated that "FERPA was not intended to prevent schools from seeking outside assistance in performing certain tasks that it would otherwise have to provide for itself."[50] As long as the task performed by the third party does not exceed the school's criteria for a legitimate educational interest, then disclosures of records to a service agent would not be outside the scope of this exception, provided that the agent was "under contract with the school to provide certain services."[51] A third party authorized by the institution may therefore be included in this exception regardless of whether the school has specifically identified the party as a "school official" in its annual FERPA notice. For purposes of this report, this exception would cover: (i) instances where a teacher or other local school official gains access to educational records in a database in order to perform his or her regular academic functions, or (ii) when a third party accesses educational records at the direction of school officials for regular academic functions, provided the third party and the educational agency have a contract authorizing such access. The second criteria means that, if a local educational institution uses a third party vendor to gather and review information for inclusion in a state database, such local institution would need a contract between itself and the vendor.

Consent is also required for disclosure when a student changes schools or applies for admission elsewhere. If the parent or student initiates the request for disclosure in a manner other than in writing, a school can send a student's educational record to another school in which the student is seeking to enroll without prior written consent.[52] In a guidance letter to Cornell University, responding to an inquiry about supplying information to a student's transfer school,

[45] *Id*. § 1232g(a)(5).

[46] *Id*. § 1232g(b)(1).

[47] *See id*. § 1232g(b)(1)(A); 34 C.F.R. § 99.31(a)(1) (2000).

[48] Advisory Letter from FPCO to the University of North Dakota (Aug. 15, 2005) (on file with CLIP).

[49] California 2004 FPCO letter, *supra* note 17.

[50] Advisory Letter from FPCO to a Parent (Sept. 7, 2004) (on file with CLIP).

[51] *Id*.

[52] 20 U.S.C. § 1232g(b)(1)(B); 34 C.F.R. § 99.34.

the FPCO stated that, "when such a request is made by a student by telephone or electronic transmission, the school should be reasonably sure that the request was indeed made by the student."[53] This exception calls for validation of the request, but not written consent if the parent or student is the requestor.

Another exception to the written consent requirement arises for educational agencies or institutions that disclose personally identifiable, non-directory information to organizations conducting studies on behalf of the educational agency or institution. To be in compliance, these studies must be conducted in order to develop, validate, or administer predictive tests, administer student aid programs, or improve instruction.[54] The agency or institution may release information without prior written consent only if the study is conducted in a manner that does not permit personal identification of parents and students by anyone outside of the research organization and as long as the information is destroyed when no longer needed for the purposes for which the study was conducted.[55] Recipients of information under this exception may not redisclose personally identifiable information outside of the research organization.[56] Under this exception a school or school district may disclose educational records to a third party vendor that such school or district has contracted with for research purposes provided that the information disclosed to such vendors remains confidential and there is a schedule for deletion of such records following the completion of the stated purpose. This exception does not permit SEAs to disclose educational records to third parties for research purposes.[57] Research contracts must be directly tied to the school or local educational institution.

Local educational agencies and their constituent schools may also disclose educational records to “authorized representatives of (I) the Comptroller General of the United States, (II) the Secretary, or (III) State educational agencies”[58] without prior written consent and for statutorily authorized purposes. The permitted disclosures are those made in connection with an audit or evaluation of federal or state supported education programs, or those made for the enforcement of, or compliance with, federal legal requirements relating to such programs.[59] Information received under this provision must be protected in a manner that does not permit personal identification of individuals by anyone except the officials listed in the regulations, “except when collection of personally identifiable information is specifically authorized by Federal law.”[60] A state educational agency may not further disclose any information provided to it under this exception in personally identifiable form to any person other than authorized representatives of such agency. The records must also be destroyed when no they are longer needed for the audit and evaluation purposes for which they were disclosed.[61]

The U.S. Department of Education and FPCO have provided detailed guidance about who is defined as an official and “authorized representative” under this exception. In a January 30, 2003 memorandum to all Chief State School Officers, the former Deputy Secretary of Education provided guidance about who may be considered an authorized representative of a state educational agency.[62] The memorandum stated that “an ‘authorized representative’ of a state educational authority must be under the direct control of that authority, *e.g.*, an employee or

[53] Advisory Letter from FPCO to Cornell University (1994) (on file with CLIP).

[54] 20 U.S.C. § 1232g(b)(1)(F); 34 C.F.R. § 99.31(a)(6).

[55] 20 U.S.C. § 1232g(b)(1)(F); 34 C.F.R. § 99.31(a)(6).

[56] 20 U.S.C. § 1232g(b)(1)(F); *see also* California 2004 FPCO Letter, *supra* note 17.

[57] *See infra*.

[58] 20 U.S.C. § 1232g(b)(1)(C).

[59] *Id.*; 34 C.F.R. §§ 99.31(a)(3)(iv), 99.35.

[60] 34 C.F.R. § 99.31(a)(3).

[61] 20 U.S.C. § 1232g(b)(1)(C); *see also* Pennsylvania 2004 FPCO Letter, *supra* note 17.

[62] Memorandum from William D. Hansen, Deputy Sec’y of Educ. to the Chief State Sch. Officials (Jan. 30, 2003), *available at* http://www.ed.gov/policy/gen/guid/secletter/030130.html (offering “[a]dditional Guidance on the Application of the Family Education Rights and Privacy Act”).

a contractor of the authority."[63] In a 2004 advisory letter to the California Department of Education, the FPCO further specified that a

> "[c]ontractor in this sense means outsourcing or using third-parties to provide services that the State educational authority would otherwise provide for itself, in circumstances where internal disclosure would be appropriate under §99.35 if the State educational authority were providing the service itself, and where the parties have entered into an agreement that establishes the State educational authority's direct control over the contractor with respect to the service provided by the contractor."[64]

This guidance approves a state department of education's use of outside contractors to perform audit and evaluation functions it would otherwise be permitted to perform itself, but the guidance does not sanction the state department of education to disclose the personally identifiable information it receives in any other situation. In 2005, the FPCO specifically addressed whether FERPA permitted a state educational agency to disclose educational records to third parties who had legitimate educational interests. The office stated:

> "There is no exception to the prior written consent requirement in FERPA that allows a State educational authority, such as CPE, to redisclose information from education records, in personally identifiable form, to outside researchers, whether or not they demonstrate 'legitimate education interest.' Educational agencies and institutions themselves may disclose education records, without prior written consent, to organizations conducting studies for them or on their behalf, for the improvement of instruction and other purposes set forth [in the regulations for the research exception]. However, this exception does not apply to a State education authority that has received information from educational records [under this exception]."[65]

Permitted disclosures for audit and evaluation purposes are significant for purposes of this report. First, statutory purposes and FCPO guidance authorize the disclosure of personally identifiable information in educational records from schools and districts to a state department of education when the state department of education is collecting the information to evaluate the state educational system and provide reports to the U.S. Department of Education under NCLB.[66] The release of records into a statewide longitudinal database for audit and evaluation purposes is permitted provided that personally identifiable information is not disclosed to anyone other than state officials or agents acting on their behalf and provided that the information is destroyed when the audit or evaluation purpose is completed.[67] This puts a durational limit on the storage of any information provided to a state agency. Unfortunately, as we discuss in our findings, most states are not in compliance with this statutory authorization because, in the absence of data retention policies, the states appear to hold information in the database indefinitely. Second, further disclosure by the state to any third party vendor is only permitted in narrow circumstances. The vendor must enter into an agreement with the state department of education, which provides that such vendor is a contractor and is under the direct control of the department.[68] Any disclosures

[63] *Id*.
[64] California 2004 FPCO letter, *supra* note 17.
[65] Advisory Letter from FPCO to Western Kentucky University (July 11, 2005) (on file with CLIP).
[66] *See* Section II.B.2
[67] 20 U.S.C. § 1232g(b)(1)(F) (2005); 34 C.F.R. § 99.31(a)(6) (2008).
[68] *See supra* note 63-64 and accompanying text.

that do not meet this criterion, or that are done simply for research purposes, are not permitted. At least one state, New Jersey, does not appear to comply with this restriction. The New Jersey contract with Public Consulting Group is between the Public Consulting Group and The NJ State Department of Treasury Purchase and Property Division rather than the Department of Education and does not indicate that the Department of Education has direct control over the vendor.[69]

Finally, investigative reports and other records created and maintained by "law enforcement units" are not considered "education records" subject to FERPA as long as the law enforcement records are maintained separately by the law enforcement unit and not by an educational unit.[70] Accordingly, FERPA does not restrict the disclosure by schools of information from law enforcement unit records to anyone, including outside law enforcement authorities, without parental consent.[71] However, information about K-12 school disciplinary actions may be disclosed without consent only if all personally identifiable information about a student has been removed, including information that would make the student's identity "easily traceable."[72] Determination of what could be considered easily traceable must be analyzed on a case-by-case basis. In making this kind of determination, the U.S. Department of Education generally considers whether a reasonable person in the educational community or a requestor who does not have specific knowledge about the student would be able to identify the student to whom the records relate without substantial additional effort.[73]

2. No Child Left Behind

NCLB requires states seeking government funding for education to create, maintain, and submit specified categories of anonymous data to the U.S. Department of Education. The Act requires states to submit an application or "plan" for improvement of their educational system and a "report card" detailing the plan's success or failure.[74] States may also choose to apply for funding under any of the many targeted initiatives in the statute, either separately or in one extensive application.[75] Each initiative must be approved by the Secretary of Education (the "Secretary") before a state receives funds and becomes obligated to fulfill certain requirements. One of the main objectives of NCLB is accountability at every level of the educational process, with the state department of education and the Secretary monitoring the progress of students and schools. In order to facilitate this monitoring, each initiative in the act requires some form of disaggregated reporting that still maintains anonymity for individual students.

The data collection requirements start with the local schools which must collect data on, among others, individual students, groups of students, teachers, parents, teaching methods, and test scores and then provide most, if not all, of that information to the local administrative agency responsible for public schools in a specified area, called the Local Educational Agency ("LEA").[76] The LEA in turn forwards the data from all of the schools reporting to it to the State Educational Agency ("SEA"), the state agency responsible for supervising the public school system. Finally, the SEA sends the information required under NCLB to the Secretary.[77]

[69] *See* Amendment No. 1 to Contract A61236 by and between Public Consulting Group and The New Jersey Division of Purchase and Property on behalf of the Department of Treasury and Department of Education, dated Aug. 31, 2005 (on file with CLIP).

[70] 20 U.S.C. § 1232g(a)(2)(B)(ii) (2005); 34 C.F.R. § 99.8 (2000).

[71] 20 U.S.C. § 1232g(a)(2)(B)(ii) (2005); 34 C.F.R. § 99.8 (2000).

[72] 34 C.F.R. § 99.3.

[73] Advisory Letter from FPCO to the Michigan Department of Education (Aug. 13, 2003) (on file with CLIP).

[74] 20 U.S.C. §§ 6301-7916 (2002).

[75] *Id.* § 7842.

[76] *Id.* § 7801(26).

[77] *Id.* § 7801(41).

Data reporting is central to NCLB, but the act does not specify how states are to collect and store the information they are required to report, or the nature of the information each level needs or should have. In fact, the act's only guidance about data collection is a specific statement that states are not authorized under NCLB to create a "nationwide database of personally identifiable information" [78] and a vague statement that they should follow existing federal laws guaranteeing civil rights.[79] The act does specifically provide that, in most circumstances, the data collected by the states or LEAs should be reported in a "disaggregated" fashion, provided that this can be done without revealing personally identifiable information.[80] NCLB therefore requires that state departments of education and the U.S. Department of Education receive information that can detail certain demographic group trends without revealing individualized information. This focus on anonymity suggests that the information required at the state level can be much less detailed and personal than many state databases currently are. Certain initiatives under the act, however, do require more specific individualized information, making it difficult for states to know how much information they need to provide to fulfill their grants and maintain their funding. This lack of significant guidance may provide one reason why many states have created statewide longitudinal databases with such large amounts of student information.

a. Title I Part A

Title I Part A of NCLB pertains to generalized educational funding provided by the federal government to the state departments of education. In order to receive any funding under NCLB, a state must satisfy the requirements of Title I Part A by completing an application or plan, implementing it if approved, and submitting an annual report card at the close of each year documenting the state's success or failure in meeting the plan's enunciated standards.[81] Schools that receive funds under this section of the Act are required to monitor the progress of their students to ensure that each one is meeting the academic objectives described in the plan.[82] The schools' progress and capabilities are then monitored in turn by the LEAs and the SEA. NCLB specifically provides that "[i]nformation collected under this section [Title I, Part A] shall be collected and disseminated in a manner that protects the privacy of individuals."[83]

The plan must describe: (i) the state's current educational standards, (ii) its new standards, (iii) how it plans to ensure that the new standards are met and that schools make adequate yearly progress ("AYP"), and (iv) how it plans to collect and report student data.[84] Each plan must also describe a method of performing yearly academic assessments of all students that conforms to certain requirements.[85] Among the numerous requirements provided for the student assessments are the following that specifically address privacy concerns: (1) the testing method must "enable results to be disaggregated within each State, local educational agency, and school by gender, race and ethnicity group, English proficiency, migrant status, disabled compared to non-disabled students, and economically disadvantaged students compared to non-economically disadvantaged students, unless such disaggregation would reveal personally identifiable information or the results would not be statistically reliable, and (2) the assessments should measure "academic achievement, knowledge and skills" objectively and not "assess personal or

[78] *Id.* § 7911.
[79] *Id.* § 6847.
[80] *See, e.g.*, *id.* § 6311(h)(1)(C)(i).
[81] *Id.* § 6311.
[82] *Id.* § 6312.
[83] *Id.* § 6311(i).
[84] *Id.* § 6311(a).
[85] *Id.* § 6311(b)(3).

family beliefs and attitudes, or publicly disclose personally identifiable information."[86] So, while states are required to collect and report assessment results for certain specified categories of students, they are not required to collect individualized assessment results at the state level. In fact, NCLB prohibits any reporting that would reveal individualized personally identifiable information.[87] However, the Act also states that: "[e]ach State educational agency may incorporate the data from the assessments under this paragraph into a State-developed longitudinal data system that links student test scores, length of enrollment, and graduation records over time."[88] There is no further guidance in the Act regarding privacy for such systems, leaving FERPA as the default rule.

One year after a plan has been implemented, a state must create and distribute an "Annual Report Card" that includes:

- aggregate information from the student assessments described above, reported by the groups mentioned above if doing so would not reveal personally identifiable information;
- a comparison between the actual achievement of students in groups compared to the objectives;
- the percentage of students not tested;
- two-year trend in student achievement in designated subject areas and grades;
- aggregate information on any other data the state collects and uses to determine AYP;
- graduation rates;
- whether LEAs are making AYP and which LEAs need improvement; and
- teacher information.[89]

Again, the act requires anonymity in the reporting phase by permitting disaggregation only if personally identifiable information is not revealed. The state may also include any other information it considers relevant, including:

- attendance rates,
- class size,
- limited English proficiency students' achievement and gains,
- incidences of violence, suspensions, expulsions or drugs,
- parental involvement,
- percentage of students completing AP courses and passing AP tests, and
- a description of the state's accountability system.[90]

Much of this information is derived from the annual report cards prepared by LEAs and given to states and the public.[91] The LEA report must include all the information in the state report, as well as schools needing improvement and a comparison of the LEA's students' achievement with those of the state as a whole.[92]

The reporting requirements of this general NCLB section do not necessitate having personally identifiable information at the state level. Disclosure of assessment results for the various demographic categories of students is in fact prohibited by the act if the disclosure is

[86] *Id.* § 6311(b)(3)(C).
[87] Id. §§ 6311(h)(1)(C)(i), 6311(h)(2)(D)
[88] *Id.* § 6311(b)(3)(B).
[89] *Id.* § 6311(h)(1)(C).
[90] *Id.* § 6311(h)(1)(D).
[91] *Id.* § 6311(h)(2).
[92] *Id.* § 6311(h)(2)(B)-(C).

likely to reveal personally identifiable information. While state departments of education do need to collect certain information about each student in order to properly report test results in the disaggregated categories, the reporting requirements do not necessitate that the state collect full personally identifiable educational records of each student.

b. Titles I-IX: Other Initiatives

NCLB includes additional sections allocating funds to states or LEAs that want to participate in certain programs or whose schools have a specified percentage of an identified group of students (e.g., Native Americans). These sections require the applications for funding to contain specified information and "such other information as the Secretary may require."[93] While most parts of these titles include the same protection against revealing personal information when disaggregating data, some sections require more detailed information concerning students, such as the correlation of test scores to the teaching method employed.[94] Several specific sections are notable for their more specific reporting requirements:

(i) Title I Part C allocates funding for the education of migratory children[95] and requires a state to include in its application a plan for facilitating the "interstate and intrastate coordination of services for migratory children" and the transfer of their health and educational records.[96] The Secretary may award separate grant money to facilitate this transfer and must assist in creating a system to link migrant students' health and educational records from each state to facilitate their electronic transfer.[97] The Secretary also must "direct the National Center for Education Statistics to collect data on migratory children."[98] This section is significant because it is exempt from the statement that NCLB does not authorize the creation of a national database.[99]

(ii) Title I Part D is called "the Prevention and Intervention Program for Children and Youth who are Neglected, Delinquent or At-Risk" and requires state agencies desiring funding to describe how they will ensure that student assessments and educational records are shared between LEAs and correctional facilities.[100] This section of NCLB is focused on coordinating the exchange of information between schools or LEAs and all other state agencies responsible for students identified as delinquent or at-risk, including correctional facilities.[101]

(iii) Title III, "Language Instruction for Limited English Proficient and Immigrant Students," allows states to apply for funding of programs for limited English speaking students provided the states have a system for reporting data concerning those students.[102] Title III also directs the Secretary to coordinate all programs serving "limited English proficient children," insure that all data collected by the U.S. Department of Education includes that of limited English proficient children, and establish a National Clearinghouse for English Language Acquisition and Language Instruction Educational Programs.[103]

[93] *Id.* § 6372.

[94] This requirement is associated with NCLB's goal to use the "best" method of teaching students. *See id.* § 6471.

[95] *Id.* §§ 6391-93.

[96] *Id.* § 6394(b)(3).

[97] *Id.* § 6398.

[98] *Id.* § 6398(e).

[99] Specifically, the act states that: "[n]othing in this chapter (other than section 6398(b) of this title [the section pertaining to funding for programs for migratory children]) shall be construed to authorize the development of a nationwide database of personally identifiable information on individuals involved in studies or other collections of data under this chapter." *Id.* § 7911.

[100] *Id.* § 6434(9).

[101] *Id.* §§ 6421, 6451.

[102] *Id.* §§ 6801 et seq.

[103] *Id.* §§ 6983(a)-(b), 7013.

(iv) Title IV, Part A, Subpart 3-Gun Possession, the "Gun Free Schools Act," requires all states "receiving federal funds under this act" to implement a State law mandating that LEAs expel for at least one year any student found to have "brought . . . or possessed a firearm at a school," with the caveat that the expulsion can be modified by the chief administering officer of the LEA "on a case-by-case basis."[104] LEAs requesting funding from the state must also report in their funding applications "the circumstances surrounding any expulsions imposed under the State law" discussed above, along with the school's name, the number of students expelled from the school, and "the type of firearms concerned."[105] The State must then report this information to the Secretary annually. In addition, LEAs will not receive funding under "any title of this Act" unless they implement "a policy requiring referral to the criminal justice or juvenile delinquency system of any student who brings a firearm or weapon to a school served by such agency."[106] States receiving funds under the act also must have implemented a procedure "in accordance with the Family Educational Rights and Privacy Act of 1974" that facilitates the transfer of these disciplinary records of expulsion or suspension from LEAs to all schools in the state.[107] While this initiative calls for more detailed reporting by states, the requirements still do not necessitate the disclosure of personally identifiable information at the state level.

C. Policy and Regulatory Influences

As a result of NCLB's reporting requirements and the general belief in the educational community that more extensive data collection can lead to better, more individualized instruction, schools and local educational agencies have begun collecting more detailed information regarding students. This locally collected information is then in turn forwarded to state departments of education for NCLB reporting purposes. As larger amounts of data are accumulated at the state level from various schools and districts, there is an increased desire to seek more efficient mechanisms for data processing. The response from both nonprofit policy groups and the U.S. Department of Education is that efficiency can best be accomplished by the development of data systems that use common interoperable data elements and codes.[108] The argument is that states will be able to process and use data better if it is reported in common formats.

Below we discuss three ways in which interoperability is being advocated in the development of state databases. First, there are two influential nonprofit organizations, the Schools Interoperability Framework Association ("SIFA") and the Council of Chief State School Officers ("CCSSO"), that have taken an active role in developing uniform standards for educational databases. The U.S. Department of Education is an active participant in both. Second, the U.S. Department of Education initiated a federal grant program, the Statewide Longitudinal Data Systems Grant Program ("SLDS"), to assist states in developing statewide longitudinal databases.

Interoperable data collection systems may, as advocates suggest, decrease costs and simplify labor, but they also raise a number of privacy concerns. Specifically, common data standards, by definition, facilitate the combination of multiple data sets into one national data warehouse of K-12 children, which in turn could be combined with data from post-secondary data systems to create an unprecedented national database of personal information. While NCLB expressly states that the statute does not authorize a "nationwide database of personally

[104] *Id.* § 7151(a)-(b).

[105] *Id.* § 7151(d)-(e).

[106] *Id.* § 7151(h).

[107] *Id.* § 7165.

[108] See SIF Association, Welcome to SIF Association, available at http://www.sifinfo.org/us/index.asp (last visited Oct. 23, 2009); Nat'l Forum on Education Statistics, Education Data Model Version 1 (PK-12) available at http://nces.ed.gov/forum/datamodel/index.asp (last visited Oct. 23, 2009)

identifiable information," the likelihood of combining information from several states becomes very real if states are using identical data elements and codes. Interoperability thus appears as a backdoor means to create a national database of children's information without express authority under NCLB to do so.

In addition, as described below, the U.S Department of Education appears to be heavily involved in the promotion of interoperability (even if only indirectly). This involvement has largely escaped public notice and scrutiny, and the lack of a privacy policy debate is a major concern. One would expect the federal government's role in the development and deployment of interoperable standards to be minimal since NCLB did not authorize a national aggregation of data and interoperability functions to make aggregation and sharing easier. Instead, the U.S. Department of Education generally has an active role in the nonprofit organizations that are advocating and developing interoperable standards. Because the Department's activity occurs in non-governmental standards setting organizations, the decisions fall outside the normal channels of the Administrative Procedures Act and escape public oversight. Likewise, state departments of education participate in the standards groups without similar transparency for the privacy debate at the state level. This non-transparent government involvement is problematic because of the public policy implications.

1. Schools Interoperability Framework Association (SIFA)

SIFA is a nonprofit organization whose members consist of school districts, 14 state departments of education,[109] the U.S. Department of Education, and over 1,400 software vendors.[110] SIFA's stated goal is to "make it possible for school administrators, teachers and other school personnel to have access to the most current and accurate data available."[111] SIFA's mission is to remedy inefficiencies of information collection systems caused by numerous data systems that lack interoperability.[112]

At the school level, a lack of interoperability means that different data entry programs are incompatible with one another, preventing the transfer of data between programs. This problem has triggered issues such as redundant data entry and increased costs. According to SIFA, without interoperability multiple school officials are forced to enter information on one system that has previously been entered by another employee on a different system.[113] For example, a teacher is often required to enter biographical information of a student into a data system. That same information, however, might have previously been needed to register the student at the school library. SIFA's goal is to help facilitate interoperability, so that the information entered by the librarian will automatically appear on the teacher's data system, saving the teacher the redundancy of entering the identical information.[114] Multiple programs that lack interoperability also lead schools to pay higher costs to ensure that all of the systems are working properly together.[115] SIFA reports that schools typically cannot afford to maintain the systems properly, and as a consequence data is often inaccurate.[116] SIFA claims that this often damages the

[109] SIF Association Member List, http://www.sifinfo.org/members-list.asp (last visited Feb. 26, 2009). State members of SIF include: Alaska, California, Delaware, Indiana, Kentucky, Maryland, Minnesota, Ohio, Oklahoma, Pennsylvania, South Carolina, Virginia, Wisconsin, and Wyoming. *Id.*

[110] SIF Association General Overview, http://www.sifinfo.org/general-overview.asp (last visited Feb. 26, 2009).

[111] *Id.*

[112] *Id.*

[113] SIF School FAQ, http://www.sifinfo.org/us/school-faq.asp (last visited Feb. 26, 2009).

[114] *Id.*

[115] *Id.*

[116] *Id.*

educational experience of the individual student, because schools must fund programs to ensure the accuracy of the information rather than fund other important educational programs.[117]

In order to address these problems, SIFA has developed an information collection protocol, the Schools Interoperability Framework ("SIF"), that: (i) defines standard formats of shared data, (ii) defines standard naming conventions for this data, and then (iii) defines the rules of interaction among software applications.[118] The common data definitions are called "data objects."[119] For example, a student's name, address, and phone number are part of the "StudentPersonal" data object.[120] There are currently more than 90 data objects, and this number is increasing as the demand for more detailed information rises.[121] Other data objects include "StudentSectionEnrollment," "SchoolCourseInfo," and "SectionInfo."[122] The uniform coding of information that SIFA members follow to input data enables seamless sharing of information. Data collected and organized in one SIF-compliant system is easily transferable to other systems that are also in compliance with SIF.

SIFA's members have also come together to create a set of vendor-neutral rules and definitions called the "SIF Implementation Specification,"[123] which "makes it possible for programs within a school or district to share data without any additional programming and without requiring each vendor to learn and support the intricacies of other vendors' applications."[124] In other words, the SIF Implementation Specification is a set of guidelines that allows vendors to create software programs that can be interoperable, eliminating many of the problems discussed above. As a trademark, SIF is sufficiently recognized and valuable that vendors pay for their products to be certified by SIFA and become members of the organization in an effort to increase their business.[125] Before becoming members, vendors' products must be certified by SIFA. The certification test consists of a thorough examination of the software program, ensuring that it is compliant with the SIF Implementation Specification and that it operates properly.[126] Only after the program passes this test does the vendor get the benefit of using the SIF trademark and advertising that it participates in the SIF initiative.[127]

Departments of education and schools also may become SIFA members and have access to SIF. States pay a membership fee of $2,500 and in turn receive the opportunity to influence the development of the SIF specification.[128] One way members influence the standard development is by participating in a SIFA work group, task force, or committee.[129] Schools must also pay a membership fee. Schools (or districts) that want to be voting members pay a $1,000 fee, whereas nonvoting members pay only $500.[130] All schools that join receive direct access to SIF implementation tools and support, and the school's name and website are linked on the SIFA site.[131]

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *How SIF Works*, T.H.E. JOURNAL, Mar. 2002, http://www.thejournal.com/articles/15899.

[122] Edustructures—SIF Integration for K-12 Education, http://www.edustructures.com/pro/sasixp.html (last visited Feb. 26, 2009). Specific definitions of these data objects are only available to members of SIFA.

[123] General Overview, http://www.sifinfo.org/general-overview.asp (last visited Feb. 26, 2009).

[124] *Id.*

[125] SIF Certification, http://certification.sifinfo.org/ (last visited Feb. 26, 2009).

[126] *Id.*

[127] *See id.*

[128] Government Benefits, http://www.sifinfo.org/govt-benefit.asp (last visited Feb. 26, 2009).

[129] *Id.*

[130] Welcome to SIF, http://www.sifinfo.org/school-get-started.asp (last visited Feb. 26, 2009).

[131] *Id.*

The U.S. Department of Education became a member of SIFA in 2003.[132] In January of 2005, the U.S. Department of Education publicly encouraged states to consider SIF certification.[133] Hugh Walkup, Director of Strategic Accountability Service for the U.S. Department of Education, issued a statement explaining that "through its membership in SIFA the U.S. Department of Education intends to support common standards in educational data systems and to assure that Department data initiatives are aligned with and reflected in SIF standards."[134] The U.S. Department of Education's National Educational Technology Plan stated in reference to SIFA that "integrated, interoperable data systems are the key to better allocation of resources, greater management efficiency, and online and technology-based assessment of student performance that empower educators to transform teaching and personalize instruction."[135] The U.S. Department of Education saw the potential in the SIF model and wanted confirmation that its goals were factored into the SIF design.

2. Council of Chief State School Officers (CCSSO)

The CCSSO is a nationwide nonprofit organization of elected and appointed[136] public officials who head departments of elementary and secondary education in all 50 states, the District of Columbia, the Department of Defense Education Activity and five extra-state jurisdictions.[137] The CCSSO expresses views on major educational issues "to civic and professional organizations, federal agencies, Congress, and the public."[138] Since 1928, the CCSSO has provided its members with professional development tools in an effort to provide "cutting edge information" to state education agencies.[139] They currently offer 25 official publications and numerous non-regulatory guidance handbooks on federal programs.[140]

In 2004, the CCSSO partnered with Standard & Poor's School Evaluation Services and the Center for Educational Leadership and Technology Corporation ("CELT") to launch the National Education Data Partnership ("NEDP"), funded by the Bill & Melinda Gates Foundation to address state data collection.[141] In 2007, The NEDP established the State Education Data Center ("SEDC").[142] The SEDC was designed to be the "leading voice on public education data" by nationally advocating "quality education data collection, standards, and use" and providing access to a free website of education data and analytic tools.[143] The SEDC established two

[132] *Id*.

[133] Press Release, SIFA, US Department of Education Recommends Integrated Data Systems via SIF Certification (Jan. 11, 2005) (on file with CLIP).

[134] Press Release, SIFA, United States Department of Education joins SIF (Apr. 24, 2003) (on file with CLIP).

[135] Press Release, SIFA, How to Save $500,000 a Year (July 11, 2007) (on file with CLIP).

[136] *See* Chief State School Officers/Method of Selection, www.ccsso.org/chief_state_school_officers/method_of_selection/index.cfm (last visited May 22, 2009) (listing which states elect their officials through partisan or non-partisan ballots and which states' officials are appointed and by whom).

[137] COUNCIL OF CHIEF STATE SCH. OFFICERS, 2005-2006 ANNUAL REPORT, *available at* http://www.ccsso.org/content/PDFs/CCSSO_Annual_Report0506.pdf.

[138] *Id.*

[139] *Id.* at 6.

[140] *See* CCSO.org—Publications, http://www.ccsso.org/publications/index.cfm?init=1 (last visited May 22, 2009) (for official publications); NCLB: Legislation, Regulation, and Guidance, www.ccsso.org/federal_programs/NCLB/3355.cfm (last visited May 22, 2009) (for non-regulatory guidance).

[141] *See* National Education Data Partnership, www.ccsso.org/projects/National_Education_Data_Partnership/index.cfm (last visited Mar. 4, 2009).

[142] *Id.*

[143] *Id.*

programs, SchoolDataDirect.org and the Coordinated Data Ask ("CDA"), along with two advisory councils to administer these projects.[144]

SchoolDataDirect.org is a publicly accessible website that displays comprehensive current and historical multi-state educational data and allows researchers to download that data directly from the website's database.[145] "It offers comparison tools, ratios, benchmarks, and performance indicators" designed to improve understanding of how money is being spent on education and where attention needs to be given to "improve performance."[146] Although the website is not designed for NCLB reporting, it is designed to assist administrators and "education leaders who work within the NCLB environment."[147]

The multi-state data found at SchoolDataDirect.org is compiled from a number of different sources.[148] School directory information such as school type, county, and Title I status is provided by the National Center for Education Statistics ("NCES").[149] Community demographic data including population, median age, and household income distribution is provided by Global Insight, Inc., a private economic, financial, and industry analyst.[150] All NCLB Annual Yearly Progress data is provided by the state departments of education.[151] The state departments of education also provide data about school environments, such as class size, teacher quality, and disciplinary actions.[152] The NCES provides the enrollment breakdowns of each school if the state departments of education do not.[153] Enrollment is disaggregated by economically disadvantaged students, limited English proficiency, gifted and talented students, students with disabilities, and migrant students.[154] All spending, revenue and tax data is provided by the U.S. Census at the district level and NCES and the National Public Education Financial

[144] *See* State Education Data Center, www.ccsso.org/projects/state_education_data_center/index.cfm (last visited Mar. 4, 2009).

[145] *Id.*

[146] *See* National Education Data Partnership, *supra* note 141.

[147] *See* SchoolDataDirect—FAQ, www.schooldatadirect.org/app/content/q/mtype=FAQ.shtml/mlvl=0/stid=-1/llid=-1/stllid=-1/locid=-1/site=pes (last visited Mar. 4, 2009).

[148] *See* SchoolDataDirect, Data Sources, http://download.schooldatadirect.org/_ddtv/DataDownloadGuideFiles/SDD_Data_Sources.pdf (Jan. 29, 2008) (listing every data element and who provided it to the website).

[149] *Id.* Directory Information also includes: Physical Location, Charter Status, County Name, District ID, Education Entity Name, County Code, Locale Type, NCES ID, School ID, State Code, and Telephone Number. *Id.*

[150] *Id.* Community Demographics also include: Adults with Bachelor's Degree, Adults with High School Diploma, Number of Households, Population Density, Population Distribution by Age, and Single Parent Households with Children. *Id.* For more information on the programs and methodologies of Global Insight, Inc., see IHS Global Insight—About, http://www.globalinsight.com/About/ (last visited May 20, 2009).

[151] SchoolDataDirect, Data Sources, *supra* note 148. AYP indicators include: Graduation Rate, Improvement Status, Overall Status, Proficiency Status, Proficiency Targets, and Accountability Measure.

[152] *Id.* Teacher Quality includes: Average Years of Experience, Percent of Classes in High-Poverty Schools Not Taught by "Highly Qualified" teachers, Percent of Classes in Low-Poverty Schools Not Taught by "Highly Qualified" teachers, Teachers holding a Bachelor Degree, Doctorate Degree, Masters Degree and less than a Bachelor Degree. *Id.*

[153] *Id.* All enrollment data is provided by the NCES or SDOEs. *Id.* The SDOEs that provide enrollment data are: California, Colorado, Georgia, Idaho, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Mississippi, Ohio, Texas, Virginia, Vermont, and Washington. *Id.* All SDOE's provide their gifted and talented enrollment; New York provides its own economically disadvantaged enrollment while NCES collects the other enrollment elements. *Id.*

[154] *Id.*

Survey at the state level.[155] Most student performance data is provided by the state departments of education.[156]

The CDA is a new collaboration between the Data Quality Campaign ("DQC") and the U.S. Department of Education. The role of the DQC in this collaboration is not surprising. The DQC is a national initiative to coordinate efforts to support the states' development of longitudinal data systems and to inform policy makers of the need for that data. The DQC was launched as part of the CCSSO's Data Summit and is supported by the Bill and Melinda Gates Foundation and managed by the National Center for Education Accountability.[157] The DQC founding partners include significant organizations in the educational community such as Achieve, Inc.,[158] Alliance for Excellent Education,[159] CCSSO, The Education Trust,[160] National Center for Educational Accountability (NCEA),[161] National Center for Higher Education Management Systems,[162] National Governors Association Center for Best Practices,[163] SIFA,

[155] *Id.* Data elements include: Capital Expenditures by Function, Debt Service, Federal Aid by Designation, Financial Reserves, Instructional Expenditures, Local Revenue, Operating Expenditures, Revenue, Salaries, State Aid, and Total Compensation. *Id.*

[156] *Id.* SDOEs provide attendance rate, dropout rate, mobility rate (number of students entering after enrollment count plus the number of withdrawals after the enrollment count divided by the enrollment count), number tested for each grade level by subject tested, and post graduate intentions. The Manhattan Institute provides the cohort graduation rate (graduation rate estimate). *Id.* The Urban Institute provides the cumulative promotion index (graduation rate estimate) and NCES provides the leaver rate (estimated four-year cohort graduation rate. *Id.*

[157] *See* Data Quality Campaign—Home, http://www.dataqualitycampaign.org/ (last visited May 22, 2009); *see also* 2005 Data Summit, http://www.ccsso.org/projects/Data_Quality_and_Standards_Project/7494.cfm (last visited May 22, 2009); Chiefline 11/30/05, http://www.ccsso.org/Whats_New/newsletters/chiefline/7544.cfm (last visited May 22, 2009).

[158] *See* 2005 Data Summit, *supra* note 157 (listing founding partners). Achieve, Inc., is a bipartisan, non-profit organization created by governors and business leaders that helps states benchmark academic standards and "improve assessments and strengthen accountability to prepare all young people for postsecondary education, work and citizenship." Achieve, Inc., http://www.achieve.org/ (last visited May 22, 2009).

[159] *See* Alliance for Excellent Education, http://www.all4ed.org/about_the_alliance (last visited May 21, 2009) (Funded by philanthropists, foundations and corporations, the Alliance for Excellent Education develops and disseminates research based policy recommendations on the use of data-driven decisions to policymakers, education and civil rights advocates, and the press.).

[160] *See* About the Education Trust, http://www2.edtrust.org/edtrust/about+the+ed+trust (last visited May 21, 2009). The Education Trust is funded by Bill and Melinda Gates and other foundations, and their goal is "to close the achievement gaps that separate low-income students and students of color from other youth." *Id.*; About the Education Trust, http://www2.edtrust.org/edtrust/about+the+ed+trust/major+funders (last visited June 11, 2008).

[161] *See* National Center for Educational Achievement/ Just for the Kids, http://www.just4kids.org/en/ (last visited May 22, 2009). NCEA is a non-profit, non-partisan organization designed to raise academic expectations and promote practices that help students succeed. It is the managing partner of DQC. *Id.*

[162] *See* Home—NCHEMS, http://www.nchems.org/ (last visited May 22, 2009). NCHEMS "is a private non-profit organization whose mission is to improve strategic decision making in higher education . . . ." *Id.*

[163] *See* NGA—The Center for Best Practices, http://www.nga.org/portal/site/nga/menuitem.50aeae5ff70b817ae8ebb856a11010a0/ (last visited May 22, 2009). NGA is a bipartisan organization of governors that "promotes visionary state leadership, shares best practices and speaks with a unified voice on national policy." National Governors Association, http://www.nga.org/portal/site/nga/menuitem.cdd492add7dd9cf9e8ebb856a11010a0/ (last visited May 22, 2009).

Standard & Poor's School Evaluation Services,[164] and State Higher Education Executive Officers.[165]

The DQC is a way for many organizations working on similar educational data system projects to coordinate their common goals. The DQC aims to build support to fully develop longitudinal data systems in every state by the end of 2009.[166] The DQC wants to promote the use of longitudinal and financial data to improve student achievement. The DQC will facilitate a national forum to ensure collaboration, develop consensus, and reduce duplication of effort by promoting, developing, and using common data standards and efficient data transfer and exchange.[167] The DQC has identified 10 essential elements for creating a successful longitudinal data system. These elements include: (a) unique statewide student identifier; (b) student-level enrollment, demographic and program participation information; (c) ability to match individual students' test records from year to year to measure growth; (d) information on untested students; (e) teacher identifier system with the ability to match teachers to students; (f) student-level transcript information, including information on courses completed and grades earned; (g) student-level college readiness test scores; (h) student-level graduation and dropout data; and (i) ability to match student records between the pre-K-12 and post-secondary systems.[168]

The CDA will provide a data collection template that "identifies the most commonly requested education data elements and their agreed upon definitions."[169] These elements are also compared to the suggested EDFacts data groups and to SIF objects before being finalized and can be downloaded from SchoolDataDirect.org.[170] States are being "encouraged" to develop databases with this template "to further reduce the burden of their data collection/reporting efforts."[171] Like the SIF specifications, the CDA is an effort to move states towards a more uniform system of data collection and, like SIFA, the CDA is a third-party program supported by the U.S Department of Education.

SchoolDataDirect.org and CDA demonstrate a common policy goal of universalizing data collection and building longitudinal databases. While these goals represent significant policy decisions, privacy concerns regarding interoperable data systems appear to be largely absent from the planning protocols and need to be addressed.

3. Statewide Longitudinal Data Systems Grant Program (SLDS)

The Educational Technical Assistance Act of 2002 created the Institute of Education Sciences ("IES") and its National Center for Education Statistics ("NCES") and authorized the

[164] *See* SchoolMatters—Home, http://www.schoolmatters.com/ (providing an objective source of information and analysis of school data).

[165] *See* SHEEO Mission & History, http://www.sheeo.org/About/mission.htm (last visited May 22, 2009). SHEEO is a professional organization of CEOs serving statewide governing and coordinating boards of higher education dedicated to promoting relationships with federal agencies, colleges and universities, and higher education and other associations in the collection and exchange of data and information. *Id.*

[166] See Data Quality Campaign, About DQC, available at http://www.dataqualitycampaign.org/about (last visited Oct. 23, 2009); Achieve, Data Quality Campaign Launched at Data Summit (Nov. 27, 2005) available at http://www.achieve.org/node/91 (last visited Oct. 23, 2009)

[167] Id.

[168] THE NAT'L EDUC. DATA SUMMIT, DATA QUALITY CAMPAIGN: IMPROVING THE QUALITY, ACCESSIBILITY AND USE OF DATA IN EDUCATION (2006), http://www.dataqualitycampaign.org/files/Presentations-NGA_FL_Data_Summitt_020206.pdf.

[169] *See* State Education Data Center, www.ccsso.org/projects/state_education_data_center/index.cfm (last visited May 22, 2009).

[170] *Id.*

[171] *See supra* note 137.

SLDS grant program.[172] The grants are designed to aid SEAs in their design, development and implementation of longitudinal data systems.[173] The grants range from one and a half million to six million dollars per state and are given for three years.[174] Grants are awarded based on the need for the project and the quality of the project's design and management plan.[175]As of June 2007, 27 states have received grants from the program.[176] All states, territories, and the District of Columbia are eligible to apply.[177] CCSSO staff, funded through a contract with NCES, supports the administration of these grants.[178]

There were 22 requirements that a state had to meet to receive a grant in 2007. The requirements notably include the following:

- the state must articulate a governance structure including the representatives who will design, develop, implement, manage, and maintain the statewide longitudinal data system;
- the state must use permanent student identifiers;
- the state must create a data warehouse to manage and store linked data that can be accessible by teachers, schools, districts, and researchers;
- the state must link the data over time to allow for longitudinal analysis of student growth;
- the state must put in place clearly defined security, access, and use policies in conformance with FERPA as well as technical procedures for protecting security, confidentiality, and integrity of data;
- the state must have an automated reporting system that ensures timely and accurate data will meet reporting requirements;
- the state must provide data, reports, and analysis through "secure-access enterprise information portals" to inform decision-making of teachers, parents, administrators, LEA, and SEA; and
- the state must develop a data exchange to share data within the state and with institutions of other states, in conformance with FERPA.[179]

Additionally, 9 "voluntary standards and guidelines" were offered to prospective grant recipients.[180] Significantly, SIF standards appear among the set of voluntary standards for grant

[172] Statewide Longitudinal Data Systems Grant Program—Program Overview, http://nces.ed.gov/Programs/SLDS/index.asp (last visited May 24, 2009).

[173] *Id.*

[174] *Id.*

[175] Press Release, U.S. Department of Education, 13 States Win $62.2 Million in Grants for Longitudinal Data Systems (July 2, 2007), *available at* http://www.ed.gov/news/pressreleases/2007/07/07022007a.html.

[176] *See supra* note 165 (14 States received grants in November 2005: Alaska, Arkansas, California, Connecticut, Florida, Kentucky, Maryland, Michigan, Minnesota, Ohio, Pennsylvania, South Carolina, Tennessee, Wisconsin; 13 States received grants in June of 2007: Arizona, Colorado, District of Columbia, Indiana, Kansas, Maine, Nevada, New Hampshire, North Carolina, Oregon, Utah, Virginia).

[177] *Id.*

[178] *See* Administrative Data Improvement, www.ccsso.org/projects/administrative_data_improvement/index.cfm (last visited Mar. 3, 2009).

[179] *See* Statewide Longitudinal Data Systems Grant Program—Archives, http://nces.ed.gov/Programs/SLDS/archives.asp (last visited Mar. 3, 2009).

[180] *See* Statewide Longitudinal Data Systems Grant Program—Voluntary Standards and Guidelines, http://nces.ed.gov/Programs/SLDS/standardsguidelines.asp (last visited Mar. 3, 2009).

> "The development of a statewide longitudinal data system requires work and preparation. To guide States in their development efforts, please use the information contained on this page to inform and shape project plans. Much of the information contained here was also

recipients, and 11 of the 13 states receiving grants in 2007 expressly mention SIF in their grant proposals.[181] The popularity of including SIF standards in a grant proposal may indicate an understanding at the state level that the U.S. Department of Education supports and advocates uniform data collection and eventual aggregation. While the grant system does require that security, access, and use policies be incorporated in the state database, other privacy concerns, such as the duration of storage and purpose limitations, are lacking.

> included in the original RFA sent out to all prospective grantees and should be heeded in future grant application efforts."

Id .(Follow the links to coding systems, NCES handbooks for data definitions, confidentiality guides, security standards, reporting regulations, SIF standards, and the National education technology plan.).

[181] *See* Grantee State Applications, http://nces.ed.gov/Programs/SLDS/stateinfo.asp (last visited May 21, 2009) (follow the links to each state to download the grant proposals). All page numbers correspond to the pdfs of the state's individual grant proposal: Nebraska pg. 16, North Carolina pg. 22, Kansas pg. 21, Colorado pg. 24, Virginia pg. 19, Indiana pg. 22, Utah pg. 17, New Hampshire pg. 31, Arizona (in partnership with Connecticut and Maine) pg. e15 and 23, District of Columbia pg. 31, Maine pg. 23. Only Oregon and Nevada do not mention SIF explicitly. Oregon does have a partnership in place that allows data transferability with Washington, but no national plans in place. Nevada has just implemented a data sharing program with higher education facilities within the state and noted that grant funds may be used to support a national system, but did not mention SIF.

III. FINDINGS

All of the states have an ongoing interest and need to maintain student longitudinal databases. Many states rely on NCLB to explain the existence of the database, stating on their websites or in letters to parents that the federal government requires them to collect information concerning students and then store it in a database. Some states, however, also assert that the database method of information gathering is more efficient, in that its automated nature should make teachers' and administrators' reporting duties easier and faster. They also argue that the database will improve the quality and usage of data by facilitating researchers' desires to learn about demographics and groups. The ultimate goal is the use of the collected data to improve school quality in each state and the country as a whole, possibly through research into the "best" way to teach students. Whatever the reason for the database, it is clear that increased data collection and use are priorities, and that best practices regarding privacy need to be incorporated into such databases.

The review of publicly available information resulted in findings that are presented in three categories. First, the findings show trends related to data collection, including how and what information is collected at the state level. Second, the findings show the various privacy protections that are applied to the state longitudinal databases. Finally, the findings show the use of third party vendors in the collection and maintenance of the student data.

A. Information Collection Practices

Thirty-eight states are collecting some type of longitudinal student data at the state level. Of the remaining 12 states, some are developing longitudinal programs and several have insufficient information available on their data practices to make an assessment. Below, we identify the common types of data collected and the reasons for its collection. Some data is clearly required to be collected by NCLB, some data appears to be collected to aid academic improvement, and other data appears to fall outside of legitimate educational purposes.[182]

It is critical to note that all of the data discussed below is collected in individualized form, even if the data is not tied directly to a name. Each data field, for example, is collected in connection to a specific record, whether that record is identified by a student name or a non-personally identifiable student number. This collection method is significant for privacy concerns, because one piece of non-identifiable information may become identifiable when linked to a second piece of information.

[182] This section should be considered in conjunction with the next section on privacy protections because regardless of the purpose, all information must be subject to effective privacy protections.

Data Summary Chart- 1

EXISTING LONGITUDINAL DATABASES

- ***States with longitudinal database (36 states):***

  AK, AZ, CA, CO, FL, GA, IL, IA, KS, KY, LA, ME, MA, MI, MN, MO, MT, NE, NH, NJ, NM, NY, NC, ND, OH, OR, PA, RI, SD, TN, TX, VA, VT, WA, WI, WY

- ***States developing a longitudinal database (5 states):***

  CT, DE, HI, IN, SC

- ***States with a longitudinal database, but without public information detailing the data processing (2 states):***

  MS & OK

- ***States with insufficient public information to determine (7 states):***

  AL, AR, ID, MD, NV, UT, WV

1. General Overview

Every state with a database collects directory information of students.[183] As noted above, this can include: "the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student."[184] Both Missouri and New York limit collection almost exclusively to directory information supplemented by a few additional data items.[185] For these states with limited data collection, privacy concerns are muted.

Almost every state assigns each student a unique identification number to identify that student without using the student's name.[186] Several states have systems in which a student receives a second identification number at the local level.[187] Each state varies with respect to the data that is associated with each identification number. Iowa, for example, only collects directory data in one system that assigns the state ID number, but collects more detailed information in

[183] *See infra* app. A.
[184] *See supra* note 23.
[185] *See infra* apps. A-G.
[186] *See infra* app. B.
[187] The following states appear to assign a second ID number at the local level: Missouri, Montana, Nebraska, New Hampshire and New Jersey.

another database using that state ID number.[188] Approximately 16 states also collect a student's social security number, and in Georgia and Louisiana the social security number usually doubles as the student's unique identification number.[189]

Most states also collect a range of demographic information relating to their students.[190] At least 36 states record the gender of an individual student and at least 35 states keep track of the race and ethnicity of their students. At least 24 states require a record on the immigration status of their students and some states have data elements for a student's country of birth, which also provides an inference of immigration status.[191] Over half the states collect data on a student's native language or the primary language spoken in a student's home. For those students with limited English proficiency, 31 states keep track of their participation in Limited English Proficiency ("LEP") programs. Twenty-eight states also include a student's migrant status.[192]

The detailed personal information collected by the majority of states extends to a student's academic record as well.[193] Every state keeps track of students' individual standardized test scores in order to report score statistics as required by NCLB. At least 18 states record which students qualify for special testing accommodations, such as extra testing time. A minimum of 15 states also maintain data on which students require extra help or tutoring with their school work. The research indicates that Colorado, Connecticut and Iowa also keep data on their students' ACT scores. Seven states collect information on whether an individual student takes AP courses and 18 states note whether a student is considered gifted or talented. At the other end of the spectrum, a minimum of 27 states keep records on special education students. Lastly, 12 states keep records on the post-graduation plans of students.

Disciplinary details relating to individual students are maintained by almost every state in various ways.[194] Twenty-six states maintain records on the reason a student withdraws from a particular school. Nineteen of these 26 states include reasons such as expulsion, jail, illness, mental health, or pregnancy as descriptors. Fifteen states collect detailed data about disciplinary actions, including the reason a specific student was disciplined and the date the disciplinary action was taken. A minority of states document the number of absences for each student, and a number of states keep track of every student's suspensions.[195]

States also track certain economic wealth factors related to students and their families.[196] An overwhelming majority of states maintain records on a student's eligibility for free or reduced price lunch. At least 25 states note whether a student is homeless. Of these states, 13 further document where the homeless student stays at night.

Lastly, a few states collect some form of health information about their students.[197] Maine and North Carolina record the Medicaid status and Medicaid numbers of applicable students. Kentucky and New Jersey both keep track of a student's most recent medical examination date. New Jersey also collects data on the date of a student's last lead test, the resulting lead level from that test, and the date of the student's polio immunization. Florida has a

[188] *See* Iowa Department of Education Data Access and Management Policy Statement For the Iowa Student Identification/Location System and Project Easier Student Records, http://www.iowa.gov/educate/index.php?option=com_docman&task=cat_view&gid=321&Itemid=1563 (last visited May 5, 2009) (follow the links to download the document).

[189] *See infra* app. B.

[190] *See generally infra* app. C.

[191] *See* the Country of Birth column *infra* app. A.

[192] *See generally infra* app. C.

[193] For information regarding academic records, see *infra* app. D.

[194] For information regarding disciplinary records, see generally *infra* app. E.

[195] At least 18 states keep records of absences, and a minimum of six states do the same for suspensions, see *infra* app. E.

[196] For information regarding economic and family information, see *infra* app. F.

[197] For information regarding health records, see *infra* app. G.

separate immunization database where health records are stored, monitoring past and upcoming immunization dates.[198] Finally, South Dakota collects the weight of students as part of its child obesity program.[199]

Overall, the information collected by the states can be broken down into two categories: (i) general data or information that is used for NCLB reporting purposes, and (ii) data that is not required by or used for NCLB.

Data Summary Chart- 2

LONGITUDINAL DATABASES AND SENSITIVE DATA

- ***32% of states collect children's social security numbers***
- ***22% of states record student pregnancies***
- ***46% of states have a mechanism in place to track children's mental health, illness and jail sentences***
- ***72% of states collect children's family wealth indicators***

2. Data Used for NCLB Reporting

Much of the data collected by the states is required or permitted to be collected in a general manner for NCLB purposes, provided that personally identifiable information is removed prior to public reporting. NCLB requires that all schools receiving funding keep track of the test scores of its students, and that states report statistics about those test scores in their annual report card "disaggregated by race, ethnicity, gender, disability status, migrant status, English proficiency, and [other statuses] such as economically disadvantaged."[200] The annual report card may also include generalized information about student attendance rates, class size, school violence, drug use and AP test results.[201] The requirements of the annual report card explain why many of the categories of information are collected at the state level; however, they do not necessitate that such information be tied to a specific student when collected by the state. Rather than collecting this information in individualized student records, states could collect numerical information generally in disaggregated categories.

[198] *See* Florida Compulsory School Immunization Update, *available at* http://www.fldoe.org/eias/databaseworkshop/word/immunization.doc (last visited Mar. 4, 2009).

[199] *See* Tracking Childhood Obesity, http://doe.sd.gov/educationonline/2007/May/art_article3.asp (last visited Apr. 2, 2009).

[200] 20 U.S.C. § 6311(h)(1)(C)(i) (2002).

[201] *Id.* § 6311(h)(1)(D).

There are also special funding programs that the states can apply for under NCLB.[202] These programs require the collection of additional information at the state level in order to receive federal funding. For such programs, states are required to keep track of migrant students, special education students, and students with limited English proficiency. All schools also must inform the local law enforcement or a juvenile facility when a student brings a weapon to school.[203] Certain disciplinary incidents likewise must be reported in a generalized aggregate fashion. These reports are not required to identify the victims of crimes or students accused of crimes. Again, these additional programs help to explain why certain general categories of information are collected at the state level, but they do not require individualized personally identifiable reporting to the state.

Although much of the data collected by the states is required by NCLB, the data need not be linked to identifiable information at the state level. The privacy protection section of this study addresses this topic in depth, but it is important to note that there are existing systems that effectively prevent the state from linking the information it receives to a specific student. Unfortunately, most states do not use these anonymizing techniques. This is especially problematic, because most states also have minimal or non-existent data retention policies, which means that the information collected in a student's education file will remain in that file for many years, even when that data is expunged from other files such as a student's juvenile criminal record.

3. Data that is unlikely to be required by NCLB

Many states gather data that appears to exceed the collection requirements of NCLB such as teen pregnancies or country of birth. While this additional data may be helpful at a school level to assist teachers in developing individualized teaching plans, there does not appear to be a strong rationale for processing this data at the state level; and, to the extent such data is collected at the state level, it does not need to be collected in an individualized fashion.

There is some data collected by states that is not required by NCLB, but there are reasonable explanations for the collection. At least 11 states keep track of whether a particular student is pregnant or a single parent.[204] Despite the intrusive nature of this information, teachers can use it to better tailor instruction for the student. For example, a feasible homework load for a student-parent may be different from that of another student. If teachers are aware of a student's situation, attention can be given as to how best to assure single parents do not fall behind. Additionally, Kansas, Minnesota, and North Carolina amass information on what mode of transportation a student uses to get to school and how many miles that student must travel each day to get there.[205] This data is not required for NCLB collection, but the time it takes for a student to get to school can be valuable information for a teacher. Similar to the time constraints imposed on student parents, a student who spends an unusual amount of time traveling to and

[202] *See Section II.B.2(b)*

[203] *Id.* § 7151(d)-(e).

[204] *See infra* apps. C, G. Arizona, Arkansas, Louisiana, Montana, New York, New Mexico, Oregon, Pennsylvania, Florida, Georgia, and Nebraska all keep track of student parents and/or pregnancy.

[205] *See* KIDS 2008-2009 Collection System File Specifications, *available at* http://www.ksde.org/LinkClick.aspx?fileticket=CfXC6hszkis%3d&tabid=2508&mid=6013; Data Element Definitions, http://education.state.mn.us/mdeprod/idcplg?IdcService=GET_FILE&dDocName=014043&RevisionSelectionMethod=latestReleased&Rendition=primary; NCWise Introduction to Student Demographics, *available at* http://www.ncwise.org/TRAINING/ncwise_training_documents/Documents/gen_stu_info/Student_Demographics.pdf (last visited May 20, 2009).

from school might have difficulty spending the necessary hours on school work. Knowledge of this information can help a teacher tailor instruction for these individuals. It is significant, however, that while this information can be helpful at the local level, at the state level the collection of this data on an individualized basis seems tertiary to the improvement of instruction.

Some states also collect data in excess of NCLB requirements that seem to lack any significant educational purpose. For example, both Maine and Michigan keep track of the birth order of students.[206] This information is not required by NCLB, and appears to be tertiary for instructional tracking. Likewise, California records the educational level of a student's parents.[207] This individualized data does not seem to be a legitimate marker for the need to improve instructional support for a public school child. Collection of non-required information such as birth order and parental education level, while ostensibly benign, sets a precedent for excessive data collection.

Most troubling however, is the collection of information that exceeds the scope of NCLB and may have a legitimate purpose for collection, but also carries a high risk of harm to the students if privacy is not sufficiently maintained. The inclusion of this type of information in a statewide database must be assessed against its usefulness for educational improvement and the risks associated with children's privacy.

The first of these problematic data categories includes elements that keep track longitudinally of a student's mental health or criminal history. For example, Iowa's data system includes a code for court action as an explanation for a student's withdrawal from school,[208] and Illinois includes a code for jail as an explanation for why a student was not tested.[209] At least 17 other states have codes for withdrawal that include jail, illness, or mental health.[210] The collection of data pertaining to the criminal justice system can be especially damaging to a student. Many states provide that juvenile criminal records can be sealed and eventually expunged.[211] However, even if the juvenile criminal records are sealed or expunged once the student reaches the age of majority, the incidents will still remain part of the student's education file in the absence of a comparable data purge requirement. Most states, however, do not have policies in place regarding data retention and data purging. Thus, this information in a student's file is extremely troubling.

Many states also include far more detailed descriptions of disciplinary incidents than required by NCLB. When a student brings a weapon to school, NCLB requires the school to refer the matter to local law enforcement officials. As part of the school record, however, ten states keep track of the specific type of weapon used. For example, Louisiana's weapon codes consist of handguns, rifles, shotguns, poisonous gas, any firearm muffler or silencer, or the frame of any weapon.[212] Louisiana goes further than many states and provides 32 different codes to detail disciplinary action, including codes for rape, murder, assault and battery, kidnapping, foul

[206] *See* MEDMS On-line User Manual–Unit 6: Maintain Student Information, https://www.medms.maine.gov/MEDMS/usermanual/unit6.htm (last visited May 25, 2009); Michigan Education Information System Single Record Student Database Data Field Description (Spring 2009), *available at* http://www.michigan.gov/documents/cepi/spr2009_SRSD_field_descriptions_258932_7.pdf.

[207] *See* Statewide Student Identifier User Guide (Version 2.2) (Sept. 29, 2008), *available at* http://www.csis.k12.ca.us/library/statewide-identifier/SSID-User-Guide-for-SB1453-v2-2-20080929.pdf.

[208] *See* Project EASIER—Iowa Department of Education, http://www.iowa.gov/educate/index.php?option=com_content&task=view&id=44&Itemid=12 (last visited Mar. 4, 2009) (follow the links to download the Data Dictionary 2008-2009).

[209] ISBE SIS Data Elements—Reason for Not Testing (Oct. 3, 2007), *available at* http://www.isbe.state.il.us/sis/pdf/not_testing.pdf.

[210] *See infra* app. E.

[211] *See* Reporter's Comm. for Freedom of the Press, Access to Juvenile Courts: State-by-State Summaries (Spring 1999), http://www.rcfp.org/juvcts/juvcts_stateindex.html (last visited October 20, 2009).

[212] *See infra* apps. E, G.

language, arson, missile throwing, burglary, and serious bodily harm.[213] Louisiana describes serious bodily harm as a bodily injury "that involves a substantial risk of death; extreme physical pain; protracted and obvious disfigurement; or protracted loss or impairment of the function of bodily member, organ or faculty."[214] Florida's disciplinary codes also include involvement in hate crimes, gang related violence or drug and alcohol use.[215] These detailed descriptions of disciplinary violations stay in the student's record for a duration that depends on the existence of a data retention policy. This level of detail also makes identification of a student much easier even if the database is structured to anonymize students. Additionally, Michigan requires that schools keep track of students who have been victims of an incident, which is explicitly not required by NCLB.[216] This may stigmatize a student as a victim throughout his or her school years.

Similarly, a number of states include more information about student disabilities than is required by NCLB. States are not mandated to disclose the type of disability that a student has. Nonetheless, at least eight states include in the database students' disability type.[217] Georgia has particularly detailed descriptions, with options ranging from "mild intellectual disability" to "severe intellectual disability," and finally "profound intellectual disability."[218] There do not appear to be clear guidelines distinguishing the characteristics of each code. Without clearer guidelines, it is possible for a student to be mislabeled by or mistreated as a result of these overarching terms.

The collection of health information that is not required by NCLB is also troubling. Congress has recognized that health records are of a particularly sensitive nature by its enactment of the *Health Insurance Portability and Accountability Act*. Every precaution should be taken to ensure their privacy. Their inclusion in education databases without special safeguards jeopardizes this goal. States do collect health related information without apparent special protections. For example, New Jersey keeps track of a student's most recent medical examination date and also collects the date of a student's last lead test, the resulting lead level from that test, and the date of the student's polio immunization.[219] While New Jersey's detailed technical guidelines provide that disclosure of this health information is optional, it is not clearly presented that way in letters to parents.[220] As a result, families may provide health information they would prefer to keep confidential, because they think disclosure is mandatory.

Lastly, Florida includes data that can be perceived as highly intrusive. Specifically, Florida keeps track of the birth weight of a student's baby (when more than 5 pounds and eight

[213] *See* SIS User Guide (ver. 8.6), *available at* http://www.doe.state.la.us/lde/uploads/7706.pdf (last visited Mar. 4, 2009).

[214] *Id.* (Louisiana Disciplinary Code Number 32).

[215] *See infra* apps. E, G.

[216] *See* Michigan Education Information System Single Record Student Database Data Field Description, *supra* note 206.

[217] *See infra* apps. D, G.

[218] FY 2008 FTE Data Collection Data Element Detail Cycle 2, http://public.doe.k12.ga.us/DMGetDocument.aspx/FTE2008_2_Data%20Element%20Detail_10_25_07.pdf?p=6CC6799F8C1371F651B228FF2DA4BFDB0B711E805EC2A08BC245DA562544D56F&Type=D

[219] *See infra* app. G.

[220] Letter from Lucille E. Davy, Acting Commissioner, Dep't of Educ. and James W. Smith, Jr., Acting Commissioner, Dep't of Human Servs. to Parents (Sept. 15, 2006), http://www.state.nj.us/education/njsmart/data/abbott_health.pdf (concerning the collection of health-related data).

ounces).[221] This data may be used to generate inferences regarding whether the mothers were using drugs while pregnant.

In general, it appears that the databases hold much more information than is required for NCLB reporting purposes. While much of the detailed information in the longitudinal databases may be beneficial for local level personnel, the level of detail required for state reporting appears to be excessive.

Data Summary Chart - 3

EXAMPLES OF EXCESSIVE DATA COLLECTED BY STATES

- ***Birth order***
- ***Birth weight of a student's baby***
- ***Victim of peer violence***
- ***Medical test results***
- ***Parental education level***
- ***Mental health problems***
- ***Criminal history***

B. Privacy Protections

Almost all of the states express an interest in protecting the privacy of their students and complying with FERPA. The states use various mechanisms to ensure the privacy and confidentiality of student educational records. First, the technical structure of longitudinal databases affects the state's ability to protect privacy and to comply with FERPA. And, second, beyond the database architecture, states use a variety of policy tools, including limitations for defined database users and uses, confidentiality agreements, FERPA required notices of data practices, and in some cases data retention policies. However, as noted throughout these findings, many states only provide obscure, incomplete, or difficult to decipher information about their data practices and programs. In itself, this lack of transparency for the state's processing of children's data is inconsistent with fair information practices and FERPA policy goals.

1. Database Architecture

The state longitudinal databases appear to use two different infrastructure forms. The majority of states have adopted a "dual" database system: one database collects a limited amount

[221] Florida Department of Education, http://edwapp.doe.state.fl.us/bsn_subjects/TargetElementDesc1.aspx?SubjectID=1&FacetID=3&ViewID=512&TableID=143&ElementID=1394 (last visited Mar. 4, 2009) (data element descriptions).

of student information in order to assign student identifiers and a separate database stores the detailed longitudinal data about each student.[222] The alternative system currently in practice is a "unified" database containing both identifying data and longitudinal data.[223] The unified databases tend to rely on access restrictions to separate various data elements from general use. Each of these systems is discussed in greater detail below.

As we reviewed the various types of databases, we considered whether the technical architecture was adequately designed to protect privacy by assessing whether the data flows in each structure supported compliance with FERPA's requirements and exceptions. As we discussed above, FERPA requires written parental consent before the disclosure of personally identifiable non-directory information unless: (i) the data is being used by the state for audit and evaluation purposes, subject to the requirements discussed above; or (ii) all personally identifiable information has been removed.[224]

The architecture that a state adopts for the use of student identifiers in the database is a key factor in the protection of student privacy and for FERPA compliance. Some type of unique student identifier ("USI") is necessary for states to implement statewide longitudinal databases. Privacy concerns and FERPA obligations depend on the link between the USI and individual students' identities. If the USI is being used generally to identify a student for multiple purposes within the state or local school district, then the reporting of educational records by the local school districts to the state database may only be made for audit and evaluation purposes, because the student identifier functions as personally identifiable information and would thus not qualify for the anonymity exception. However, when an institution successfully creates a non-personally identifiable USI that is used specifically for reporting information from the local educational agency to the state, that data reporting qualifies as a permitted disclosure of 'anonymized' data; all other personally identifiable information is withheld. An important element in ensuring the USI is an anonymous identifier to qualify for the permitted disclosure is whether state level employees can trace a USI to a specific student. Anonymity can only be accomplished when state level employees have no access to the linking key between the USI and the personally identifiable information, and no way to infer the identity of a specific student from the available data.

The permitted disclosure of anonymous information to the state for non-audit and evaluation purposes also depends on whether the data flows into the state database system operate to prevent re-identification of individual students. A statistical disclosure and, thus, re-identification arises when the number of students in a dataset or with a specified characteristic is small enough to permit re-identification of a single individual. For instance, in a search of the state assessment scores of minority students, a particular school might report information to the state that corresponds only to one student. It would not be hard to ascertain the identity of that student whose entire assessment information is publicly available. The disclosure by the local school district to the state would violate FERPA unless the disclosure to the state was made in compliance with the audit and evaluation exception. Re-identification is a major risk for disclosures related to any small number of children. Statistical cutoff procedures must be applied to ensure confidentiality.

The NCLB reporting obligations require safeguards to limit statistical disclosures of individual student information. NCLB, for example, requires states to report information disaggregated by subgroup (e.g. race, gender) unless the disaggregation would result in a

[222] It appears that the following states use this architecture: Arkansas, Arizona, California, Colorado, Georgia, Illinois, Kansas, Michigan, New Hampshire, New York, Ohio, Rhode Island, South Carolina, and Texas.

[223] It appears that the following states use this architecture: Louisiana and Nebraska.

[224] *See supra* note 46.

statistical disclosure.[225] To prevent the inadvertent reporting of personally identifiable information, it is necessary to have a minimum subgroup size. NCLB allows the states to set the cutoff for minimum subgroup sizes. The National Assessment of Educational Progress of the federal Department of Education uses 62 students as the minimum size reporting group to avoid statistical disclosures and the National Center for Education Statistics, the federal entity charged with collecting and analyzing data related to education, reports that the majority of states use subgroups ranging from 25 to 45 students as the minimum number for statistically reliable results."[226] This approach also needs to be used when local school districts report student information to a state database for purposes other than the state's audit and evaluation of programs. Nevertheless, with such a small subgrouping, re-identification will remain a serious issue.

a. Dual Database Systems

Dual database systems collect student information in two separate databases. Most commonly, states use one database to collect demographic information in order to generate a USI and a second database to hold student records longitudinally for state access.[227] The most common USI system requires the state employee or agent to enter a set of demographic data into the first database for the generation of a USI. An algorithm or random number generator then converts each student's demographic data into an assigned, unique number. As part of the USI generation process, the system uses the demographic data to verify that each student only has one USI by checking for matches with existing records. This matching process is used to assure record-keeping accuracy for the educational data. The USI is then used, instead of other identifiable information such as student name or birth date, to link student records longitudinally in the second database.

The dual database architecture tries to limit the personally identifiable information contained in the database that is accessed by state officials. Some of the dual database systems are more successful than others at anonymizing student information. Many states, though, seem to assume that use of a USI (instead of other demographic information) protects privacy. However, in many instances, the USI itself remains personally identifiable information under FERPA because of an incomplete separation between the identifier and the individual student's identity and records. In addition, statistical disclosure often remains an issue. For example, if someone at the state level is able to trace a USI backwards to the local level or into the USI database in order to discover the identity of a specific student, the USI is personally identifiable. In such instances, the release of records to the state officials must comply with the requirements of the audit and evaluation exception of FERPA.

In reviewing the dual database systems, the states appear to use three types of architecture. In the first type, the state maintains both the USI database and a separate database for the student records. [228] For this structure, local school officials transmit or input the demographic data into the state's USI database and into the state's longitudinal database. This processing is a disclosure of personally identifiable children's data. As such, FERPA allows this

[225] 20 U.S.C. § 6311(h)(1)(C)(i) (2002).

[226] NAEP Analysis and Scaling – Minimum School and Student Sample Sizes for Reporting Group Results, http://nces.ed.gov/nationsreportcard/tdw/analysis/summary_rules_minimum.asp (last visited June 30, 2009); UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, NO CHILD LEFT BEHIND ACT—IMPROVEMENTS NEEDED IN EDUCATION'S PROCESS FOR TRACKING STATES' IMPLEMENTATION OF KEY PROVISIONS 14, http://www.gao.gov/cgi-bin/getrpt?GAO-04-734 (last visited June 30, 2009).

[227] It appears that the following states use this architecture: Arkansas, Arizona, California, Colorado, Georgia, Illinois, Kansas, Michigan, New Hampshire, New York, Ohio, Rhode Island, South Carolina, and Texas.

[228] Vermont, Kansas, Texas, and Georgia appear to use this type of system, *see infra* app H.

disclosure only for audit and evaluation purposes and only if the criteria established for these purposes are met, including deletion of the data at the conclusion of the audit or evaluation.

In the second type of dual database architecture, the USI is assigned at the local level while the longitudinal database with student record data is maintained at the state level.[229] States that use this design still typically permit state officials to have access to the local USI database in order to verify the information in the longitudinal database. As a result, the longitudinal data held by the state is personally identified because state officials can trace children's records back through the USI database to identify specific students. Consequently, this architecture would, under FERPA, limit the disclosure by local schools of the student records to audit and evaluation purposes.

While these dual database architectures as presently designed seem to qualify only for audit and evaluation uses, the states that have implemented these architectures do not appear to meet the procedural requirements under FERPA. FERPA requires that the data be deleted once the audit and evaluation programs are completed.[230] Our review revealed that most states do not have any apparent data retention policies nor any apparent procedures for data deletion. In addition, these basic architectures of the student databases do not appear to limit the uses of the data to audit and evaluation purposes.

In the third type of dual database architecture, some states take a further step in the design of their system and seek to create a firewall between personally identifiable information and the state's longitudinal database by using third parties to generate the USI numbers.[231] The FERPA summary above discussed the guidance the FPCO has provided agencies and institutions implementing these systems to ensure the creation of a non-personally identifiable USI.[232] This guidance essentially outlines three requirements that should be in place before a USI tied to an educational record is considered anonymous and, therefore, within the "non-personally identifiable" exception of FERPA:

(i) the USI must be something other than a scrambled social security number or student number, unless the USI is protected by "written agreements reflecting generally accepted confidentiality standards within the research community" and only those with "access to the linking key" would be able to link a student to their record;

(ii) the data from the records may only be released "in a manner that ensures that the identity of any student cannot be determined, including assurances of sufficient cell and subgroup sizes;" and

(iii) the key that links the USI to identifiable information "is itself an education record subject to the privacy protections of FERPA" and it must not be shared with anyone outside the "agency or institution."[233]

The states opting for this design (using third parties to generate the USI) seek to create the necessary boundary between the linking key and the children's personal information so that the

[229] Arkansas, Arizona, California, Colorado, Illinois, Michigan, Ohio, New Hampshire, Rhode Island, South Carolina, and New York appear to use this type of system, *see infra* app H.

[230] 20 U.S.C. § 1232g(b)(3)(C).

[231] Arizona, California, New Hampshire, Ohio, Rhode Island, and South Carolina all have the separate databases used to create the USI that are maintained by third parties, *see infra* app H. There may be other states who also utilize a separate third-party maintained database system but this information was often difficult to obtain publicly.

[232] *See* Section II.B.1(a).

[233] *See supra* note 30.

data reported to the state's separate longitudinal database can qualify as "non-personally identified" data in terms of FERPA.

When states create USI numbers that qualify as non-personally identifiable numbers, local school districts may report student data to the state database without parental consent.[234] Under these conditions, the state's use of the data is not limited to audit and evaluation purposes. When this advisory guidance is not followed, however, the USI may still be personally identifiable information and, as such, would still be subject to the requirements of FERPA unless the audit and evaluation exception applies.

For the majority of states, their adherence to the "linking key" guidance in the creation of the USI numbers is unclear. [235] Our research of publicly available information determined there are only three states, New Hampshire, Kansas, and Ohio, that appear to be adhering to FPCO guidance on rendering data non-personally identifiable.[236] Additionally, New York removes student names and the unique identifiers are encrypted when school records leave the local level.[237] The 10 additional states that collect demographic data exclusively for USI purposes seem to utilize systems that may be able to comply with FPCO guidance, but either all of the protections are not in place or the specific details of their system are not available.[238]

As examples of effective architectures, New Hampshire and Ohio have each contracted with third parties to develop and maintain their USI databases.[239] For these states, the third parties generate the USI and the local school districts anonymize the student record data before reporting the data to the state. Procedurally, the local school district sends a student's demographic data, via a web based application, to the third party. The third party then generates and reports the USI to the local school district. This USI is then used, instead of any other personally identifiable information, when sending assessment data to the longitudinal database. In turn, state officials gain access from the longitudinal database to records using only the USI, and statistical measures are in place to ensure that the child's information is not personally identifiable. This architecture means that only school personnel at the local level know which USI is linked to an individual student. Additionally, only the third-party generating the USI would know the "linking key" between the demographic information and USI. In the New

[234] If, however, the data reporting results in a statistical disclosure of children's identities, then the restrictions on personally identifiable data will apply.

[235] Most states and local school districts appear to follow the second prong of the FPCO guidance with respect to statistical samples and use sufficient group sizes to limit statistical disclosures of personally identifiable information, but it is not clear whether most states conform with the rest of the FPCO guidance.

[236] New Hampshire, Kansas and Ohio apparently adhere to the FPCO guidance; California and Illionois seem to be in the process of developing this type of system as well. *See, e.g.*, Application for Grants Under the Statewide Longitudinal Data Systems (Mar. 15, 2007), *available at* http://nces.ed.gov/Programs/SLDS/pdf/Kansas.pdf (Kansas's application for grants); ODE—2003 EMIS Manual, http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEDetail.aspx?page=3&TopicRelationID=1101&ContentID=12084&Content=50921 (last visited May 25, 2009); ODE—Statewide Student Identifier, http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEDetail.aspx?Page=3&TopicRelationID=3&Content=60670 (last visited May 25, 2009); Policy and Procedures Manual for i4see and Related Data (Sept. 4, 2007), *available at* http://www.ed.state.nh.us/education/datacollection/i4see/NH%20i4see%20Policy%20Manual%20v080220.doc.

[237] NY State Student Identification System User Guide, Version 5.4 (Dec. 29, 2006), *available at* http://www.emsc.nysed.gov/nysstudents/nyssisguide.doc.

[238] *These states are:* Arkansas, Arizona, California, Colorado, Georgia, Illinois, Michigan, Rhode Island, South Carolina, and Texas.

[239] For details on these USI and longitudinal databases, see ODE—2003 EMIS Manual, *supra* note 236; ODE—Statewide Student Identifier, *supra* note 236; Policy and Procedures Manual for i4see and Related Data, *supra* note 236.

Hampshire and Ohio models, the third party is bound by a confidentiality agreement to not share any personally identifiable information to which they are exposed, including the "linking key."[240] This appears to conform to the FCPO guidance on anonymization. In effect, this structure seeks to assure that the state only maintains a database containing non-personally identifiable information, assuming that the proper statistical disclosure rules are in place before any information is sent on to the state level.

Whether most states adopting dual database architectures have structured their systems to enable compliance with FERPA is unclear, because there is only limited information available on how most states manage their USI databases and grant access to them. Generally, the only information available is that a separate USI system exists. For example, Indiana provides information about FERPA, but does not explain how the state's system is in compliance with the act.[241] Likewise, Georgia makes no mention of any privacy protections or how the state's USI system functions.[242] South Carolina, however, says the state will securely keep all personally identifiable information in an USI database and no other state agency will have access to that database.[243] It is often unclear, however, how the USI is generated and who maintains access to the linking key. In these cases, if anyone at the state level has access to the linking key, then the USI is considered personally identifiable information and the state's access to and use of the educational records must conform with the audit and evaluation exception.

Nevertheless, a properly structured dual database system seems to be a viable option for enabling anonymization. All personally identifiable information is maintained separately from assessment data and can be easily subjected to heightened security precautions. Furthermore, personally identifiable data is only relevant while a student is attending school so that their USI can be matched and verified. Once the student is no longer within the educational system, the personally identifiable data and the USI linking key should be expunged. While individual assessment data may be useful to educators and researchers for many years after a particular student leaves the educational system, there is no reason for that data to remain linked to the student. The dual database system allows states to develop specific data retention policies that require personally identifiable information to be removed regularly while assessment data could remain until no longer needed.

[240] California is also in the process of developing this type of system, see *infra* app H.

[241] *See* Balancing Student Privacy and School Safety: A Guide to the Family Educational Rights and Privacy Act for Elementary and Secondary Schools, *available at* http://www.doe.in.gov/stn/pdf/FERPA.pdf (last visited May 25, 2009).

[242] *See generally* Georgia Department of Education—Data Warehouse, http://www.doe.k12.ga.us/pea_infosys.aspx?PageReq=DataW (last visited May 25, 2009).

[243] *See* South Carolina Department of Education SCEDS and SUNS Data Access and Management Policy, *available at* http://ed.sc.gov/agency/Accountability/Technology-Services/Documents/5-3DraftDataAccessPolicy.pdf (last visited Mar. 4, 2009).

Data Summary Chart – 4

ANONYMIZING DATA: DUAL DATABASE STRUCTURES

- ***Only 6 states appear to use a third party who restricts the state's access to the student ID numbers (i.e. prevents state access to individual student data)***
- ***4 states store both the student ID numbers and the longitudinal database at the state level (i.e. allows state access to individual student data)***
- ***11 states store the student ID numbers locally but allow state employees access (i.e. allows the state access to individual student data)***

b. Unified Database System with Access Restrictions

States that rely on the unified database architecture maintain a single database that contains all of a student's personally identifiable information and assessment data.[244] States adopting this approach attempt to protect personally identifiable information by controlling who may access specific data. In the unified database models, access restrictions are imposed for specific data elements in an attempt to ensure confidentiality of personally identifiable information.

In the unified database architecture, the state assigns an access level to each data element in the database. A user is allowed access to the levels of data in accordance with the user's role. This means that the entire student record is not available to the user; rather, the user may only access the elements in the record that are relevant to the user's authorized activity. While there is still a need for a mechanism to preclude statistical disclosure, states that use this system maintain that the levels are designed to maximize use by educators without risking additional inappropriate disclosures to the state or public.

In such a system, for example, every data element might be assigned an access level between 1 and 3. In this example, level 1 data is the most protected and would include personally identifiable information. The level 1 data would only be accessible at the local school level. This would allow school administrators to accurately verify a USI, correct, change or make additions

[244] Arizona, Florida, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Nebraska, Nevada, New Jersey, Pennsylvania, Tennessee, Virginia, West Virginia, and Wyoming do not have any information on a separate database for USI, see *infra* app H. However, some of these states have contracts with vendors who design and implement USI systems. It is unclear whether the USI is generated separately and then input into the single database, or if there are multiple databases that we were unable to find during our research.

to the student's record, and share the record among all of the students' teachers. Level 2 data would be all data that needs to be aggregated for reporting. This would include race, gender, and assessment scores, but not personal information, like telephone numbers, that is only needed at the local level. The level 2 data would be available to a small number of administrators at the state department of education and access would be limited for "audit and accreditation" purposes only. While it would be possible in certain instances to identify a student by analyzing a combination of these data elements, the USI would ordinarily be the only personally identifiable information accessible to the state administrators. Level 3 data would not include any personally identifiable information and would be accessible to all officials at the state level in addition to parents and other educators.

In our review of states using unified database architectures, it was unclear who defines the access levels. In general, the detailed functioning of these systems was not disclosed in publicly available information. It often appeared that the access levels were defined by the state department of education, but it was unclear whether access permissions were authorized for each user by the state or by a local educational agency employee. It was also unclear what types of uses were granted to each access level. Importantly, in many instances, permissible use of the data did not appear to be addressed in the definitions of the access levels.

States using this approach, nevertheless, have their own variants. For example, Nebraska uses a unified database system with access controls.[245] Nebraska assigns every data element in the system an access level between 1 and 3, with level 1 being the most protected data. Level 1 data is likely to include the entire school record including personally identifiable information and assessment data. In Nebraska, Level 1 access is given to the state department of education staff where "a minimal number of staff will be given access to all the information in the database."[246] State access to this personally identifiable information seems counterintuitive and problematic under FERPA. It would seem that access for the personally identified data should be found at the local level rather than at the state level. Nebraska uses their Level 2 access for "audit and accreditation" and states that only some state department of education staff will have access to a limited set of data. The Level 3 access in Nebraska is reserved for district and school personnel and limits their access to individual records. Although we could not find specific details regarding these limits, they are probably determined by a role based system.

2. Other Key Privacy Protections

There are a number of ways, in addition to database structure, that states are attempting to protect the privacy of students' records. Good privacy protections at both the local and state level include defining users and specified, legitimate purposes of use, requiring confidentiality agreements for individuals who handle student records, developing specific data retention policies, and making information about FERPA rights and obligations available and accessible to parents.

[245] *See generally* Nebraska Data Access and Management Policy, *available at* http://www.nde.state.ne.us/nssrs/Docs/NE_Data_Access_and_Management_Policy505.doc (last visited Mar. 4, 2009).

[246] *Id*. South Carolina, Kansas, and Iowa have similar language regarding who at their respective DOE has access to the database, see *infra* app H.

Data Summary Chart - 5

EXISTENCE OF KEY PRIVACY PROTECTIONS

- ***Only 18 states have detailed access and use restrictions***
- ***Only 18 states require database users to enter into confidentiality agreements***
- ***Only 10 states have data retention policies***
- ***49 states make FERPA information accessible on the Internet, but for many the information is hard to find, vague or incomprehensible.***

a. Defined users and specified, legitimate purposes of use

Eighteen states[247] have some type of detailed access restrictions outlined in their materials. The remaining 24 states that we reviewed merely make a generalized reference to FERPA when discussing who can access records and for what purposes. Defining users and specifying the permissible uses of the database are essential to protect privacy in both dual and unified database architectures. Access can be assigned based on a user's role, a student's enrollment, or may be assigned after an application process. The failure to include access and use restrictions puts children's privacy at risk.

Users should be school officials with a legitimate educational interest. A "school official with a legitimate educational interest" is defined by the NCES as: (i)"a person employed by the agency or school in an administrative, counseling, supervisory, academic, student support services or research position, or a support person to these positions[;]" and (ii) "[a] person employed by or under contract to the agency or school to perform a special task."[248] Interestingly, the NCES also stated that "protection of privacy and data accuracy are essential to any data coordination efforts. However, these protections do not have to be absolute barriers to data coordination . . ."[249]

Role based access typically allows a user to access children's records when the user has a legitimate educational interest in the records. Some states use these restrictions to protect children's privacy in addition to having a separate USI database.[250] Specifically, a superintendent

[247] Arkansas, California, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Massachusetts, Michigan, Mississippi, New Hampshire, Ohio, Pennsylvania, Rhode Island, South Carolina, South Dakota, and Virginia.

[248] NATIONAL CENTER FOR EDUCATION STATISTICS, PROTECTING THE PRIVACY OF STUDENT RECORDS: GUIDELINES FOR EDUCATION AGENCIES 58 (1997), http://nces.ed.gov/pubs97/97527.pdf.

[249] *Id.*

[250] California, Iowa, Illinois, Kansas, Montana, New York, and South Carolina, *see infra* app H.

may see all of the data collected about any of the students in the school district; a principal may see all of the data collected from students in the principal's school; and a teacher may see all of the data related to the teacher's students. For example, in New York, the state defines four levels for data set elements and access depends on the nature of the data and ranges from school-based to statewide.[251]

Similarly, Illinois has different access levels for the "general user" and the "administrator." The general user can place online requests for new student identifiers for an individual student and search for existing student identifiers and student enrollment records.[252] The administrator has access to all the functions of the general user plus the ability to change student demographic, enrollment/exiting, and participation indicator data after a student identifier has been assigned.[253]

Enrollment access allows a user to access data of those students who are enrolled in the user's class, school, or district. Although these enrollment and role-based access systems are similar, enrollment access appears to be more specific and ensures that access to an individual record will be prohibited when a student transfers out of a class, school, or district.

Application based access is assigned after a user submits an application to access the database. States will often require an authorized official to control access.[254] That person will give permission by providing a username and password to access the database. Information about the typical application process and approval authority was not generally available. In four of the states that use this process, the applicant must sign a confidentiality agreement in addition to receiving the approval of a school official.[255] However, we could not find specific information on what factors the school officials use to approve an applicant or the eligibility criteria for applications. This safeguard appears to be problematic because the descriptions of access and use limitations are very general. For example, some states merely declare that only appropriate users will have access, while other states indicate that access will be granted in accordance with FERPA.[256] The vagueness of these policies suggests that application based access is a weak protection for children's privacy.

In addition to defined users, processes need to be in place for approving uses beyond the original purposes of the database. There are two ways that agencies can release data to researchers in compliance with FERPA: (i) a local school district can grant specific research rights; or (ii) the state can release non-personally identifiable information. The majority of states either do not have detailed processes for approving researchers' use of data or do not make that information easily available. A few states, however, have developed detailed processes for granting specific research rights when third party researchers or other users want to access data. For example, before disclosure in New Mexico, parental consent must be given and the parents must specify the records to be released, the reason to release them, and identify the groups or

[251] *See* New York State Student Information Repository System (SIRS) Manual—Reporting Data for the 2008-2009 School Year 24-25 (2008), *available at* http://www.emsc.nysed.gov/irts/SIRS/2008-09/2008-09SIRS-MANUAL-4-1.pdf.

[252] ISBE Student Information System User Manual, http://www.isbe.state.il.us/sis/html/user_manual.htm (last visited Oct. 22, 2009).

[253] *Id*.

[254] Arkansas, Illinois, Mississippi, South Carolina, (superintendent controls access), California (requests for access reviewed by LEA and CDE staff in a "procedure"), Kansas (requires district approval), Massachusetts (applications managed by Directory Administrators), Virginia (local account manager grants access), see *infra* app H.

[255] Illinois, Kansas, Mississippi, and South Carolina, see *infra* app H.

[256] *See* Kansas, New Mexico, New Hampshire, New Jersey, Pennsylvania (in accordance with FERPA), Iowa, Michigan, Pennsylvania, Rhode Island, South Dakota (only authorized users will have access), see *infra* app H.

individuals who will receive the records.[257] Likewise, Kansas has a very detailed policy for disclosure to researchers that includes review by a "data request review board." of a researcher's proposal. Additionally, if a proposal is accepted, the researcher must sign a confidentiality agreement.[258]

b. Confidentiality Agreements

Eighteen states explicitly mention that they require confidentiality agreements to be executed by users of the state database.[259] For example, in Iowa, system users must sign an assurance statement covering system usage before they are given access to the system.[260] The Illinois vendor contract with IBM states that all third parties to whom information is disclosed must sign confidentiality agreements and all employees and subcontractors with access to student record information must sign confidentiality agreements as well.[261] Additionally, when the Kansas Department of Education discloses personally identifiable information of students to organizations for research and analysis purposes, the recipient organization must sign an Acknowledgment of Confidentiality Requirements.[262]

In some of these states, the confidentiality agreements are mandated by statute.[263] For example, Ohio users are bonded against unauthorized use and release pursuant to state law.[264] The confidentiality agreements, however, are typically directed at personally identifiable information and do not necessarily pertain to the USI linking key.[265] Throughout the course of our research we found that only New Hampshire and Ohio assert that the USI linking key is protected and will never be released to the state level education agency.[266] These are the only two states explicitly adhering to the first and third prong of the FPCO guidance regarding an USI linking key. If there are specific confidentiality agreements for those with access to linking keys in any other states, agreements do not appear to be publicly available.

[257] Student – Teacher Accountability Reporting System Volume 2 Reference Materials 2007-2008, *available at* http://www.ped.state.nm.us/stars/dl09/SY2009%20STARS%20MANUAL-VOLUME%202.pdf (last visited Mar. 4, 2009).

[258] *See* KSDE Data Access and Use Policy—Personally Identifiable Student Information (2006), http://www.ksde.org/LinkClick.aspx?fileticket=ndfZ%2bqai7vQ%3d&tabid=2508&mid=6013 (last visited May 24, 2009).

[259] Illinois, Iowa, Kansas, Louisiana, Michigan, Mississippi, Montana, New Hampshire, New Jersey, North Carolina, Ohio, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, West Virginia, and Wisconsin, see *infra* app H.

[260] *See* State ID Policy Assurance Statement, *available at* http://www.iowa.gov/educate/index.php?option=com_content&task=view&id=1&Itemid=1264 (last visited Mar. 6, 2009) (follow the links to download the statement).

[261] Contractual Agreement Between Illinois State Board of Education and International Business Machines Corporation (on file with CLIP).

[262] Kansas Individual Data on Students - Answers to Parents' Questions (Apr. 2005) (on file with CLIP) [hereinafter Kansas Answers to Parents' Questions].

[263] *See* Ohio, Minnesota, Montana.

[264] *See* OHIO REV. CODE ANN. § 3301.0714(k) (2008), *available at* http://codes.ohio.gov/orc/3301.0714.

[265] Kansas, Louisiana, Michigan, Mississippi, Montana, New Jersey, Pennsylvania, South Carolina, South Dakota, and Wisconsin have general confidentiality agreements for individuals accessing school records; Iowa, New Hampshire, North Carolina, Ohio, Texas, and West Virginia have more specific confidentiality agreements relating to users of the ID database, see *infra* app H.

[266] Only Ohio and New Hampshire have this information publicly accessible. *See* FY2003 EMIS Guide, Appendix L—Student Identifier (SID), http://www.ode.state.oh.us/GD/DocumentManagement/DocumentDownload.aspx?DocumentID=12603 (last visited May 26, 2009). California and Kansas may also have this policy, but it was not clear from publicly available materials, see *infra* app H.

c. Data Retention Policies

Only ten states provide a detailed data retention policy for the state database.[267] This small number is significant because student information could potentially be held in these data warehouses indefinitely. A data retention policy should limit the duration of storage of educational records and inform students, parents, and data warehouse users how long data will be kept. For example, North Carolina states that data is kept for two years after the graduation or withdrawal of a particular student.[268] North Dakota recommends the retention of data for four years.[269] In addition, Connecticut maintains a detailed records retention schedule but does not clearly require the purging of historical information. Instead, the policy requires certain records to be kept for a minimum of six years.[270] Montana's data retention policy is required by statute.[271] In Montana, the school district is obligated to inform parents when personally identifiable information is no longer needed to provide educational services to the student. Following this notification, parents may request the information be destroyed, but a permanent record of the student's enrollment must be maintained.[272]

Thirty-two states had no data retention policy listed, or described very generally when data would no longer be stored.[273] For example, when describing record retention, Kansas broadly states that "information will be destroyed in a manner that protects confidentiality when information is no longer needed."[274] In West Virginia, directory and grade information are kept in perpetuity.[275]

The many beneficial reasons for maintaining detailed historical databases are beyond the scope of this study. However, it is important to note that, while the retention of historical data can be beneficial, the legitimacy of the state retaining personally identifiable information is highly doubtful.[276] Accordingly, all personally identifiable information, including USI's, should be cleansed from databases as early as graduation or the termination of education or when no longer needed for legitimate educational purposes.

[267] Colorado, Connecticut, Michigan (authorizes deletion but does not require), Minnesota, Missouri, Montana, North Carolina, North Dakota, South Carolina, and Texas, see *infra* app H.

[268]

[269] *See* STATE OF NORTH DAKOTA DEPARTMENT OF PUBLIC INSTRUCTION, 2008-2009 LEA AND SCHOOL FALL REPORTS AND DIRECTORIES 2 (2008), http://www.dpi.state.nd.us/resource/ORS/mis/mis01_02_instr.pdf.

[270] *See* Bob Lichtenstein, *FERPA & Record Keeping Powerpoint Presentation*, Oct. 2005 (on file with CLIP).

[271] MONT. CODE ANN. § 20-2-212 (2007); Montana Local Government Retention and Disposition Schedules X, XIII (on file with CLIP).

[272] *See* 34 C.F.R. § 300.573 (2000); MONT. CODE ANN. § 20-1-213 (2007).

[273] Arizona, Florida, Georgia, Kansas, Nebraska, New Hampshire, New Mexico, West Virginia (general or undefined retention schedule); Arkansas, California, Delaware, Illinois, Indiana, Iowa, Kentucky, Louisiana, Maine, Massachusetts, Mississippi, New Jersey, New York, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Vermont, Virginia, Washington, and Wisconsin (no retention policy publicly available), see *infra* app H.

[274] Kansas Answers to Parents' Questions, *supra* note 262. Nebraska and New Mexico also utilize this broad "no longer needed" language.

[275] W.V. State Board of Education Policies, Article 1 Policy 4350 §126-94-11 (on file with CLIP).

[276] There are an increasing number of states that are attempting to maintain a longitudinal database through the completion of post-secondary education. These states may contend that personally identifiable information should be retained indefinitely because some students do not pursue higher education immediately after the completion of high school (Arizona, California, Delaware, Florida, Indiana, Louisiana, New Hampshire, North Carolina, Rhode Island, and Vermont).

d. *Availability of information related to FERPA rights and obligations*

FERPA requires that educational agencies provide information to parents regarding their rights under FERPA and give information to parents regarding the parents' right to review and correct errors in their child's educational records. This notification requirement gives parents greater control over the disclosure of their children's educational records. Since state departments of education are gathering and holding student educational records, we examined how they complied with this notice requirement. We specifically looked at the state education department websites, since that is often where information regarding the state database is found and that is where many parents are likely to turn if they have questions regarding the database and their rights.

Forty-nine states had FERPA information accessible on their websites. Alabama was the only state that did not seem to have any FERPA information available. In both Montana and Nebraska, FERPA is consistently referenced on the websites, and these states explain how their data warehousing policy is in compliance with FERPA. In Montana, the policy states that parents are to be told of their rights under FERPA whenever relevant.[277] In Nebraska, specific sections of FERPA are cited extensively throughout the website.[278] Similarly, Florida has detailed protections listed in their website materials of how they protect student information in accordance with FERPA.[279]

While most states do provide FERPA information to parents, some are more accessible than others. For example, Kansas offers, via their website, a conspicuous notice to parents of FERPA rights.[280] Similarly, Montana constantly compares the state's policies to the FERPA requirements.[281] Other states provide the FERPA notices on their websites, but the information can only be found if one is specifically looking for it. For instance, on the Rhode Island website, the information could only be located by typing "FERPA" into a search field because it was buried in a legal section on the website that would not be an obvious place for parents to look.[282]

C. Third Party Vendors

1. Vendor Contracts

Most states appear to use third party vendors ("vendor") for some portion of their longitudinal data collecting and reporting needs. Some vendors market packages primarily for consulting services and assistance in data driven decision making, while others supply software and hardware for a state's entire data collection and analysis program. The range of vendors included: Big 5 Data Centers, Claraview, Inc., Cognos Business Solutions, Controltec, Inc., Deloitte Metadata Solutions, Education Statistics System Workbench, My Consulting Group, Regional Information Centers, Public Consulting Group, SAS Institute, Inc., Third Day Solutions, Wen-GAGE, and X-Wave. However, Infinite Campus, Computer Power Solutions of Illinois (CPSI), eScholar, IBM, and ESP Solutions Group were used with a notable frequency among the states and will be discussed below in greater detail.

[277] *See* Montana Office of Public Instruction, http://opi.mt.gov (last visited May 26, 2009).
[278] *See* http://www.nde.state.ne.us/ (last visited May 26, 2009).
[279] *See* Florida Depatment of Education, FERPA, http://www.fldoe.org/ese/ferphome.asp (last visited May 26, 2009).
[280] *See* Kansas State Department of Education, Data Access and Use Policy, *available at* http://www.ksde.org/Default.aspx?tabid=83 (last visited Oct. 20, 2009).
[281] *See* Montana Office of Public Instruction, Student Records Confidentiality Policy, *available at* http://www.opi.state.mt.us/ (last visited May 26, 2009).
[282] *See* http://www.ride.ri.gov/commissioner/legal/ferpa_ppra.aspx (last visited Oct. 20, 2009).

While some states use a single vendor for a specific task, others use a combination of vendors to satisfy the scope of their needs. The vendors' services are marketed separately to both local and state educational agencies. Our review, however, is focused primarily on statewide vendor agreements. Such agreements are required under FERPA to be between the vendor and the state department of education and to provide that the vendor is under the direct control of the department of education for the specific purposes of providing audit and evaluation services.[283] Additionally, most vendors offer customizable service packages and options to suit the needs of any education entity. As a result, two service contracts are rarely identical, even when the same vendor is involved.

Below, we have highlighted the general privacy or security provisions found in the contracts between six states and their respective vendors. These six states are representative of the statewide development contracts that we were able to identify from publicly available information. When it appeared from the publicly available information that a state department of education used a third party vendor to provide full statewide database development services, we requested a copy of the vendor contract from the department of education. Requests were sent to several states, but only the contracts received from the six states below appeared to be full statewide development agreements. Additional states may have statewide development agreements, but such information either was not publicly available or the state's response to our inquiry did not produce such an agreement.

a. Illinois State Board of Education (ISBE)

ISBE contracted with IBM for the development of a statewide longitudinal data system to satisfy NCLB requirements.[284] The contract states that ISBE retains IBM "as contractor" to "design, develop, implement, and document" the system and co-manage it with ISBE.[285] Although we were not provided with the contractual exhibits setting forth the database specifications, it appears from the contract and its amendments that IBM develops the system's operational software and stores the database on its servers. Employees at each local school district send student information to the database via a web application. IBM then produces anonymous state IDs and provides assessment data to state level employees. Details regarding access and use restrictions or storage duration were not available in the documents we reviewed.

The agreement recognizes that IBM will come in contact with confidential student information and acknowledges the need for compliance with "the relevant requirements [of FERPA].[286] To further protect privacy, the contract requires IBM to "limit access to student education records to those employees who reasonably need access to them in order to perform their responsibilities" and also requires each employee execute a confidentiality agreement.[287] In order to ensure compliance with this confidentiality clause, the agreement also requires IBM to keep an access record of all of its employees that access the database.[288]

[283] *See* Memorandum from William D. Hansen, Deputy Secretary of Education to Chief State School Officers, Additional Guidance on the Application of the Family Education Rights and Privacy Act (Jan. 30, 2003), *available at* http://www.ed.gov/policy/gen/guid/secletter/030130.html; California 2004 FPCO letter, *supra* note 17.

[284] Contractual Agreement No. my05211 by and between Illinois State Department of Education and International Business Machines Corporation, dated July 14, 2004, as amended, p.1 [hereinafter the Illinois-IBM Agreement No. my05211] (on file with CLIP).

[285] *Id.*

[286] *Id.* at 8.

[287] *Id.*

[288] *Id.*

b. Kentucky Department of Education (KDE)

The KDE provides an example of a state dividing some of the processing functions for its database across multiple vendors. KDE contracted with Infinite Campus to furnish hardware and software for the statewide student information system.[289] Separately, KDE contracted with Claraview, Inc. to develop a web interface that would provide general assessment information to the public.[290]

Under the Infinite Campus contract, Infinite Campus provides servers to store the database and develops the software for the system.[291] Infinite Campus also supplies the data dictionary and the training for staff that is needed to implement the project.[292] The agreement and attachments do not specify obligations for Infinite Campus to apply particular security, access or use restrictions to the database.

Under the contract between KDE and Claraview, Claraview agreed to develop a web application for the display of student reports. The terms of the agreement require that Claraview's web interface be "accessible by a variety of different system stakeholders including parents, teachers, [and] school administrators."[293] While the detailed specifications of this project were not provided, it appears that the Claraview application will interface with the database stored by Infinite Campus and take data from the database to generate assessment reports for the general public. The only clause related to privacy in the agreement itself states that "[a]ll Federal and State Regulations and Statutes related to confidentiality shall be applicable to the Contractor."[294]

c. *Montana Office of Public Instruction (MOPI)*

MOPI also contracted with Infinite Campus for the development of "a state-level Data Warehouse, Student Information System and Special Education Records Information Management System that would be accessible to the State Education Agency and all Local Education Agencies within the State of Montana."[295] Like the Kentucky system, it appears that the database would be located on Infinite Campus servers. The contract does not set forth precise specifications for the database system. Notably, the agreement does not include any specific privacy or security clauses.

d. Maine Department of Education (MDOE)

MDOE contracted with Xwave to develop a state level database, the Maine Education Data Management System (MEDMS), in order to receive student records from each local school district's student information system.[296] The contract provides that MEDMS and the local

[289] Master Agreement No. MA 758 S-06137527 by and between Kentucky Department of Education and Infinite Campus, dated Dec. 1, 2006 [hereinafter the Kentucky Infinite Campus Agreement] (on file with CLIP).

[290] Master Agreement No. MA 758 0700001487 by and between Kentucky Department of Education and Claraview, Inc., dated June 1, 2007 [hereinafter the Kentucky Claraview Agreement] (on file with CLIP).

[291] Kentucky Infinite Campus Agreement, *supra* note 289, at ¶ 4.

[292] *Id.* at attachment A.

[293] Kentucky Claraview Agreement, *supra* note 290, at 1.

[294] *Id* at 8.

[295] Contract No. OPI-1203O by and between Montana Office of Public Instruction and Infinite Campus, as amended, 5 [hereinafter the Montana Infinite Campus Agreement] (on file with CLIP).

[296] State of Maine, Department of Education Agreement to Purchase Services, Agreement No. 1202270, by and between the State of Maine, Department of Education and Xwave New England Corp., dated Mar. 18, 2003, 3 [hereinafter the Maine-Xwave Agreement No. 1202270] (on file with CLIP).

systems that furnish the student records are required to use the SIF data formats.[297] Under the contract, Xwave agrees to develop a database system in accordance with specifications set forth by MDOE. The agreement was unclear with respect to the location of the data warehouse, namely whether Xwave servers would store the data and provide access to the MDOE through an internet connection or whether Xwave would develop the system to reside on MDOE servers.[298] The development agreement did not specify any time limitations on data storage.

The agreement does set forth some general and specific privacy, security, and access guidelines to be incorporated into the database. The general clause states that MEDMS security and confidentiality protocols shall comply with Maine Department of Education Regulations, Chapter 125.[299] Section 12.01 of Chapter 125 provides generally that a school board shall develop policies in accordance with FERPA, that "records shall be entrusted to designated personnel who shall be knowledgeable about the confidentiality provisions applicable to the records," and that "all records shall be safeguarded from unauthorized access."[300] The database must also generally comply with the State of Maine's Information Technology Security Policy.[301]

The contract also sets forth more specific access and security measures that must be included to protect the database. First, the database must have role-based access restrictions for state level employees, such as "Organizational Administrator, Administrator, and System Administrator."[302] Each access role type must be limited to perform tasks only within segmented areas of the database. For example, a specific role type may have read only access to some data elements, read and modification access to another set of data elements and no access other data elements.[303] Second, the database must also be structured to have role-based access restrictions implemented for employees at the local level, including teachers, school administrators, and superintendants.[304] Both the access and actions permitted to these groups will depend upon their role (e.g. teachers will have the ability to enter and change information but can only see records of their specific students, a superintendent will have access to numerous records, but may only be permitted to view certain records). The contract requires that a system log record the access and use restrictions granted to users.[305] Additionally, the contract contemplates that these access levels will change based on a student's enrollment. For example, if a student has multiple teachers, each would be able to access that student's records. If the student then moves to a new school, only the teachers at the school in which the student is presently enrolled would have access to the student's records.[306]

e. New Jersey Department of Education (NJDOE)

New Jersey has outsourced the development of its data warehouse program. In January 2005, the New Jersey Division of Purchase and Property entered into an agreement with Public Consulting Group ("PCG") for consulting services related to its Special Education Medicaid Initiative ("SEMI") and Medicaid Administrative Claiming ("MAC").[307] This agreement with

[297] *Id.*

[298] The specifications provide that the database is to be made accessible through a web connection, but it is not clear whether the database itself would be stored locally on the MDOE servers or offsite on the Xwave servers., see The Maine-Xwave Agreement No. 1202270, *supra* note 296.

[299] The Maine-Xwave Agreement No. 1202270, *supra* note 296, at 4.

[300] Maine Department of Education Regulations Chapter 125, § 12.01 (on file with CLIP).

[301] Maine-Xwave Agreement No. 1202270, *supra* note 296, at 4.

[302] *Id.* at 5.

[303] *Id.*

[304] *Id.* at 6.

[305] *Id.* at 5.

[306] *Id.* at 7.

[307] Contract No. A61236, dated Jan. 5, 2005. This original contract was not provided to us.

PCG was later amended by the Division of Purchase and Property on behalf of the Department of Treasury and the Department of Education[308] to include development of a data warehouse and special education record system.[309] Because FERPA requires that agreements related to data processing for program audit and evaluation purposes be under the control of the state department of education, New Jersey's contractual arrangements appear to violate FERPA. In addition, New Jersey's agreement claims that the statewide longitudinal database would "enhance the SEMI and MAC projects."[310] With this assertion, the contract provides that the costs of developing the data warehouse will billed to the SEMI and MAC reimbursement programs.[311] In other words, New Jersey is funding the statewide database with a diversion of federal medicaid funds designed to assist special needs children.

The PCG contract provides that the database will be stored on PCG servers and will use 75 data elements and 300 assessment elements.[312] The database will be accessible via a secure web-browser with different reports available to "several levels of users."[313] Specific access restrictions and security measures, however, were not set forth in the contract amendment or any of the accompanying documentation. PCG claims to have "invested hundreds of thousands of dollars to ensure top notch security"[314] and to "ensure[s] that all client information remains confidential,"[315] but more detailed security provisions are absent from the contract.

f. Tennessee Department of Education (TDOE)

TDOE contracted with SAS Institute, Inc. (SAS) to conduct analyses for student assessment and to assist in satisfying the state's reporting needs.[316] SAS was chosen to "conduct analyses of raw test scores" and "provide electronic reporting . . . of schooling effects resulting from analyses of tests."[317] Under the terms of the contract, TDOE will provide test results to SAS each year for analysis and report generation.[318] SAS will host the assessment reports on their servers and the reports will be available to the public and TDOE employees via a web interface on the TDOE website.[319] Reports "which are required by state statute" will be publicly available, however, "other analytical results useful for diagnostic purposes" will be made available "on a restricted access basis."[320] The agreement specifies that the Commissioner of Education will determine who is permitted to have restricted access. This limited group granted special access will be able to review reports on projections regarding whether students are on track with state

[308] While the Department of Purchase and Property entered this contract on behalf of the Department of Education, the contractual party with control over PCG is the Department of Purchase. This contractual situation may not be in compliance with FERPA. *See supra* notes 63-65 and accompanying text.
[309] Amendment No. 1 to Contract A61236 by and between Public Consulting Group and The New Jersey Division of Purchase and Property on behalf of the Department of Treasury and Department of Education, Aug. 31, 2005 [hereinafter the PCG Agreement Amendment] (on file with CLIP).
[310] *Id.* at 1.
[311] *Id.* at 3.
[312] Memorandum on EDSmart.EasyIEP Scope of Work (June 6, 2005) (on file with CLIP).
[313] *Id.*
[314] Public Consulting Group, *EasyIEP Background*, 2 (on file with CLIP).
[315] *Id.* at 17.
[316] Contract No. FA-05-16315-01 by and between the State of Tennessee, Department of Education and SAS Institute, Inc., dated Jan. 1, 2005, as amended [hereinafter the Tennessee SAS Agreement] (on file with CLIP).
[317] Amendment No. 1 to Tennessee SAS Agreement at 1 [hereinafter SAS Amendment] (on file with CLIP).
[318] *Id.*
[319] *Id.* at 2.
[320] *Id.*

goals or on individual student test results. The agreement states that "contractor agrees to act reasonably to prevent unauthorized access but makes no warranty or guarantee regarding impenetrability of the server(s)."[321]

2. Prominent Vendors

The vendors most frequently used throughout the states include: Infinite Campus, CPSI, eScholar, IBM, and ESP Solutions Group. With the exception of IBM, all of these vendors participate in the SIF certification program.[322] This means that the data sets developed by these vendors will be interoperable.

Infinite Campus, CPSI, and eScholar each offer systems that assist in data collection and offer services for data analysis. IBM is primarily used for data collection and storage services, while ESP specializes in data analysis and SIF compliance. Below is a summary of these major vendors and the products they are currently offering.

a. Infinite Campus

Infinite Campus has been developing internet-based student information systems since its inception in 1993.[323] Infinite Campus is SIF certified,[324] and its products are used in many districts around the country at the local level for data collection and are used by four states to fully integrate state and local tracking.[325] The company manages records on more than 3 million students. [326] Infinite Campus's business model is based on the goal of streamlining administrative tasks in order to allow more school resources to be devoted toward "planning and instruction." For example, a student's performance data is only entered into the database at the school level once. The information then automatically populates the fields made available to both district and state agencies responsible for reporting that data. All entities that need the data have the ability to access it as soon as it is first entered into the database, and teachers and schools do not have to input the data multiple times or separately send it to various reporting units.[327]

Infinite Campus recently announced the development of a National Records Exchange (NRE) that will "route student data records between K-12 customer districts."[328] This exchange will be able to take place "between two Infinite Campus districts regardless of location."[329] This means that the company is actively striving to link state databases together to form a national database of children or regional databases of children. The founder and CEO of Infinite Campus

[321] *Id*.

[322] SIF Certification—Certification Register, http://certification.sifinfo.org/cert_prodlist.tpl (last visited May 26, 2009) [hereinafter SIF Certification Register].

[323] History: Infinite Campus, Inc., http://www.infinitecampus.com/pages/company_menu/history.php (last visited May 26, 2009).

[324] *See* SIF Certification Register, *supra* note 322.

[325] Company: Infinite Campus, Inc., http://www.infinitecampus.com/pages/top_menu1/company.php (last visited May 26, 2009). States using the fully integrated State Edition are: Kentucky, Maine, Montana, and South Dakota. *Id.*

[326] *Id.*

[327] Mission, Vision and Goals: Infinite Campus, Inc., http://www.infinitecampus.com/pages/company_menu/mission-vision-goals.php (last visited May 26, 2009).

[328] Press Release, Infinite Campus, Infinite Campus Announces Nationwide District-to-District Student Data Transfers (June 9, 2008), *available at* http://www.infinitecampus.com/media/PDF%20News/20080609%20PR%20National%20Records%20Exchange%202009%201%20Announcement.pdf.

[329] *Id.*

says the National Records Exchange results in "streamlining administrative processes . . . on a national level," by reducing the time spent enrolling new students.[330] The program advertising makes no mention of privacy protections, a silence that reflects at least inadequate transparency and at worst the absence of any adequate protections. Data transfers, however, must be requested by the student's new school, and that request must be approved by the former school before the transfer takes place.[331] Participation in the program is voluntary and it will be available to all customers in the 2009 release.[332]

b. Computer Powers Solutions of Illinois

Computer Powers Solutions of Illinois (CPSI) claims to be the "leading K-12 data integrator in the country" and the "leading provider of SIF solutions in the US and Canada."[333] For more than 20 years, CPSI has helped districts develop, deploy and manage their data networks.[334] The company's clients include the state departments of education of Oklahoma and South Carolina, as well as "hundreds of school district clients in nearly every state and province in the US and Canada" providing student data accounting for over four million students.[335] CPSI is SIF certified and is committed to "make it easier for teachers to teach."[336]

c. eScholar

eScholar was founded in 1997 and provides services associated with "collecting, cleansing, identifying, analyzing and reporting" the data needed to improve education.[337] The products are SIF certified and eScholar serves on SIF Boards.[338] Eleven states and 3,400 districts use eScholar's student identification solution, Uniq-ID.[339] The Uniq-ID system is a web-based application that randomly assigns a unique identifier and uses directory information to match students to their assigned numbers.[340] When an administrator registers a student, the administrator enters that student's directory information into the Uniq-ID system. If the student's directory information is similar to a student already in the database, then a list of those registered students with similar attributes will be provided to the system administrator. The system administrator then must review the preexisting registered student's information and either match the new student with an existing ID or have a new ID assigned.[341] This provides the state with a

[330] *Id.*
[331] *Id.*
[332] *Id.*
[333] *See* CPSI, Ltd.—Home, http://www.vcasel.com/ (last visited Mar. 3, 2009).
[334] *Id.*
[335] *Id.*
[336] *See* CPSI, Ltd., About Us, http://www.vcasel.com/Company/AboutUs/tabid/85/Default.aspx (last visited Mar. 3, 2009); SIF Certification Register, *supra* note 322.
[337] *See* What eScholar Is, http://www.escholar.com/what/what.php (last visited Mar. 3, 2009).
[338] SIF Certification Register, *supra* note 322.
[339] eScholar: Where it is used—States, *available at* http://www.escholar.com/where/where_states.php (last visited May 26, 2009). The following states use the Uniq-ID system: Georgia, Iowa, Kansas, Kentucky, Missouri, Nebraska, New Mexico, New York, Pennsylvania, South Carolina, Wyoming. *Id.*
[340] eScholar Uniq-ID for Students Version 6.0, http://www.escholar.com/files/Student%20Uniq-ID%206.0%2020080331.pdf (last visited Mar. 3, 2009).
[341] *Id.*

"comprehensive and unified view of a student's multiple records" and eliminates the possibility of multiple IDs for individual students.[342]

eScholar is also the subcontractor for a program developed by the the U.S. Department of Education called the Migrant Student Information Exchange (MSIX) that allows states to "exchange migrant student records nationally."[343] MSIX is designed to "reduce the educational disruption and other problems that result from repeated moves"[344] when migrant students change schools in a single year. The system avoids the need to transfer records by hard copy.

d. IBM

IBM offers both hardware and software as well as management services. IBM has a product called a "state reporting toolkit" that is designed to "streamline data collection and storage."[345] The IBM product creates a statewide student ID that allows districts to assign and access a unique identifier for each student in the district. It also provides a state level student data repository which is called a "state student data model." The toolkit helps state education departments develop data reports and implement data reporting requirements. Lastly, this product includes a completely automated system that states can use for "extracting, approving and automatically moving data from the district [data warehouse] to the state's [data warehouse]."[346]

IBM has also worked extensively on anonymizing student record data. For example, the Ohio Department of Education (ODE) contracted with IBM to develop a Statewide Student Identifier (SSID) that would give them "the ability to track personally unidentifiable student progress across time and schools, and to determine the impact of Ohio public school programs on student success."[347] One of the key objectives of this system was to maintain the confidentiality of personal data.[348] IBM and ODE developed a system where all personally identifiable information was separated at the district level from the data the state needed to satisfy federal reporting requirements. The system was structured to exclude users without special security privileges from entering personally identifiable data at the school or district level via a website connected to the SSID database. The "stand-alone" SSID database is maintained by Pricewaterhouse Cooper and is separated from other ODE databases. Authorized users access the SSID database through a website and enter "a few data elements" at which point the system generates a SSID. The minimal information required to generate the SSID "will not be accessible by ODE or any other entity or individual."[349] It is only used to validate or request new student IDs and share enrollment and withdrawal information across school districts. The remainder of student information is then collected in a database on an IBM server and is tied only to the unique anonymous student ID. Before information is released from the database to the ODE for analysis and data-driven decision making, all personally identifiable information is removed from the

[342] Press Release, eScholar, eScholar Technology to be Foundation of US Education Department's Migrant Student Information Exchange (Oct. 30, 2006), *available at* http://www.escholar.com/news/news_MSIX.php.

[343] *Id.*

[344]

[345] *See* IBM Education Solutions, http://www-03.ibm.com/industries/education/doc/content/solution/1059989210.html (last visited Mar. 3, 2009).

[346] *Id.*

[347] *Id.*

[348] *Id.*

[349] FY2003 EMIS Guide, Appendix L—Student Identifier (SID), http://www.ode.state.oh.us/GD/DocumentManagement/DocumentDownload.aspx?DocumentID=12603 (last visited May 26, 2009).

student file. This purge includes a procedure to eliminate statistical disclosure.[350] This system allows for longitudinal reporting data to be stored at the state level without any personally identifiable information leaving the district.[351] Additionally, ODE has implemented a "secure user authentication" system that provides and controls secure access to data.[352]

IBM's SSID project with Ohio illustrates the existence of vendor products that build anonymity and confidentiality of personally identifiable student records into the database systems. IBM is currently implementing similar systems in Illinois and California.[353] However, it is unclear whether other states have or are adopting the Ohio SSID product model. For example, North Carolina contracted with IBM to manage "detailed information for 1.3 million active students enrolled in the public schools" and "maintain historical records . . . if a student returns for adult continuing education."[354] The system connects 2,250 public schools and records basic demographics, immunizations, extracurricular activities, special accommodations of standardized tests, discipline and suspension records, and performance data.[355] Information regarding the privacy protections specifically afforded to this system are not clear from the North Carolina Board of Education website, but they do reference a statewide information security policy.[356]

e. ESP Solutions Group

ESP Solutions Group advertises that it developed the "concept of 'data driven-decision making'" 30 years ago and now assists states in those data-driven decisions.[357] ESP is an adviser to the U.S. Department of Education and works to document the states' ability to report data for the U.S. Department of Education's Education Data Exchange Network (EDEN).[358] EDEN is the set of educational statistical reports gathered from state agencies by the U.S. Department of Education.[359] ESP helps states identify "gaps between their data standards and the federal requirements."[360] ESP currently helps the states calculate and evaluate academic year progress

[350] *See* SSID Project RPF, *available at* http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEDetail.aspx?page=3&TopicRelationID=3&ContentID=11215&Content=50913 (follow the links to download the file).

[351] Ohio SLDS Application Profile (June 28, 2005), *available at* http://nces.ed.gov/Programs/SLDS/pdf/Ohio.pdf ("at no time shall a district release the crosswalk that matches the SID [permanent unique identification number] with other student level data (e.g., name, address, social security number)").

[352] *Id.*

[353] Press Release, IBM, State Schools Chief Jack O'Connell Announces Selection of IBM to Develop Student Achievement Data System (Jan. 2, 2008), *available at* http://www.espsolutionsgroup.com/news/IBM_CA_010208.pdf.

[354] *See* IBM Education Solutions, http://www-03.ibm.com/industries/education/doc/content/solution/1059989110.html (last visited May 26, 2009).

[355] *Id.*

[356] *See* Statewide Information Security Manual, http://www.scio.state.nc.us/SITPoliciesAndStandards/Statewide_Information_Security_Manual.asp (last visited May 6, 2009).

[357] About ESP Solutions Group, http://www.espsolutionsgroup.com/aboutus.php (last visited Mar. 3, 2009).

[358] This program was formerly known as the Performance Based Data Management Initiative (PBDMI).

[359] ESP Client Map, http://www.espsolutionsgroup.com/clients.php (last visited Mar. 3, 2009).

[360] *Id.*

reports as well as performance benchmarks.[361] ESP also offers services to design and deploy SSIDs.[362]

ESP recently partnered with IBM to develop a new system for the California Department of Education (CDE). This system, the California Longitudinal Pupil Achievement Data System (CALPADS), includes a non-personally identifiable SSID.[363] The California Department of Education is currently developing a privacy policy for CALPADS to address FERPA requirements. It will be "a comprehensive policy for privacy, confidentiality and information security."[364] SIFA has certified ESP application products and the management team "strongly supports the SIF initiative by serving on their board of directors, co-chairing their technical board, and leading innovative statewide SIF integration projects."[365] ESP is currently providing SIF consulting to Wyoming and Ohio.[366]

[361] *See* Education Technology Consulting Services, http://www.espsolutionsgroup.com/solutions_dataanal.php#calculate (last visited Mar. 3, 2009).

[362] *Id.*

[363] *See supra* note 347.

[364] *See* California SLDS Application Profile, *available at* http://nces.ed.gov/Programs/SLDS/pdf/California.pdf (last visited Mar. 3, 2009).

[365] *See* Education Technology Consulting Services, *supra* note 361.

[366] ESP Client Map, *supra* note 359.

IV. RECOMMENDATIONS

In this section, we provide some recommendations for best practices and for legislative reform related to the collection, use, and maintenance of children's educational records. These recommendations reflect the principles of *privacy*, *transparency*, and *accountability*. These principles, taken together, address the needs and concerns of students and parents while allowing teachers and state and local school officials to access necessary information.

- ♦ *Privacy* means maintaining the confidence of all personally identifiable information; restricting access to and use of student information; and limiting information collection to necessary categories of information.

- ♦ *Transparency* means disclosing publicly the information collected, its use and the protections afford to it; making information easy to find and navigate; and providing clear information about legal rights and duties.

- ♦ *Accountability* means maintaining accurate records of access to and use of personally identifiable information; establishing formal procedures for granting third party access to student information; and publicly disclosing mechanisms for change or complaint.

A. Best Practices

The recommendations set forth below are designed to establish minimum baseline standards. Stronger and more specialized privacy protections can always be added and are advisable.

<u>Recommendation 1 – States should implement Dual Database Architecture</u>. We strongly recommend the use of the dual database structure with clear distinctions made between the local level database and the state level database. For this mechanism to be effective, a third party should maintain the linking key between the local database and the state database. Teachers and local school officials may have a legitimate educational interest in personally identifiable information, but such individualized information is not generally needed at the state level. The dual database structure permits local access to needed information while minimizing the privacy risks that arise when personally identifiable information is further distributed to individuals at the state level.

From the research, we identified two major purposes for state level collection and review of children's educational records: (i) compliance with NCLB reporting requirements, and (ii) performance evaluation of schools. Neither of these justifications for data collection requires that personally identifiable information be provided at the state level. NCLB's reporting requirements expressly prohibit the public disclosure of personal information, and performance evaluations can usually be done by examining general trends rather than information pertaining to any specific student. Privacy is easiest to maintain when disclosure is limited to a small number of people. Since we find that state information uses do not require the disclosure by local school districts of personally identifiable information, we would advise that a dual database system be used to limit disclosure of such information.

One significant way to limit the disclosure of personally identifiable information is the anonymization of student data records so that they are not traceable to an individual child. The first step in this process is the creation of a unique non-personally identifiable ID that can be used to transmit general information without transmitting identifiable information. Such unique IDs, however, are only effective if they cannot be linked to a specific student by the party using the information. For this reason, a third party should be used to generate the unique ID numbers, redact the personally identifiable information and pass the redacted information onto the state level officials. Use of a third party is most effective because third parties may be placed under contractual obligation to maintain the privacy of the linking key, thereby ensuring that personally identifiable information is not passed to state officials.

The second step to ensure anonymity is to prevent the ability to re-identify or statistically disclose a child's identity in the state level database. As we saw in states such as Ohio, having a third party buffer zone between local and state level databases is necessary in order to remove any information that may inadvertently identify a specific student. Like the linking key, this process is probably best done by a third party who can be placed under contractual obligation to prevent statistical disclosure to the best of their ability. A third party will likely have more resources and technological expertise to ensure such disclosure does not occur.

Recommendation 2- States that outsource data processing should have comprehensive agreements that explicitly address privacy obligations. When states outsource the collection or management of children's educational records to vendors, FERPA requires that the processing take place under contract with the state department of education. In order to assure that children's privacy is adequately protected when outside vendors are handling the data, states should include explicit clauses in vendor contracts that impose restrictions on access and use, set out the obligations of confidentiality, require physical and access security, and define the duration of data storage. The contractual provisions should also specify the standards to be applied for each of these obligations (e.g. level or type of encryption, etc.)

Recommendation 3 – States should limit data collection to necessary information. The data that is collected in a longitudinal database should be limited. Each state must carefully review the data that it collects and match the collection to a clear and necessary purpose. Much of the information found in the longitudinal databases we reviewed was not required to be collected by law. Information that is highly personal or sensitive, or that may become sensitive in the future, should only be collected if the purpose is compelling and narrowly tailored. While many states suggest that large data collection is necessary to improve individual instruction, we would strongly suggest that information of a highly private nature be withheld from state electronic databases. The risk of security breaches and misuse is too large to justify the collection of sensitive information in an electronic record.

Recommendation 4 – States should have specific data retention policies and procedures. In order to prevent misuse of data, there should be a clear policy in place for the deletion of personally identifiable student records after students exit the system or after the records are no longer necessary for the purpose giving rise to the initial data collection. We recommend that data other than student transcripts be deleted or anonymized no later than five years after graduation or five years after withdrawal, whichever comes first. Student data may be useful after graduation or withdrawal in order evaluate teaching methods, but it also poses a risk of misuse and unauthorized distribution. As the length of time from graduation increases, the data's usefulness for research likely decreases, while the risks stay the same or increase. In order to ensure the privacy of student information, the data should be deleted from the system. At a minimum it is suggested that all personally identifiable information other than student transcript data be deleted from the local level database, but as a precaution we would also recommend that the student data be deleted from the state level database as well.

Recommendation 5 – States should explicitly provide for limited access and use. Access to and use of both the local level database and the state level database should be limited by clear rules and technological measures. Rules should articulate which classes of state and school personnel will have access to the database, what information each class may access, when they may access information, and how the information may be used. These rules should be enforced against each user by requiring the execution of confidentiality agreements that clearly outline permitted access and use. Technological measures, such as access codes and firewalls, then need to be used to ensure that the rules are implemented.

At both the local and state level, rules about when information may be accessed and how it may be used should be clear and precise. Currently, most states use the "legitimate educational interest" test to determine when access is permissible. While this is the broad standard articulated in FERPA, we recommend that states create clearer guidelines about what constitutes a legitimate educational interest so that this rule is not abused. Providing specific guidelines about what constitutes a legitimate educational interest will eliminate doubt and help hold administrators accountable when new uses of information are proposed.

At the local level, where personally identifiable information is stored and used, access rules need to be clearly articulated. There are generally two classes of individuals who will need access to information in the database. The standards for what each class of user may view and do within the database should be different. The first group, school administrators, likely needs the broadest range of access to information, since they have an educational interest in all of the students under their supervision. The second group, teachers, only needs access to the records of the students currently enrolled in their classes. The system should incorporate technological measures that distinguish between these two groups and limit access accordingly.

At the state level, access and use rules should also be clearly defined. Although the dual database structure should limit the disclosure of personally identifiable information, it is recommended that access be granted only to a small working group at the state level. There should be clear use restrictions in place for this group, such as NCLB reporting or evaluation of a specified educational program or school during a specified time. Clear purposes and timelines for use of the data will enable better accountability at the state level.

Recommendation 6 – States should maintain audit logs that track system use. We recommend implementing an audit log system to track use of the database and access to student information. Maintaining adequate records of system use is an important step in preventing data misuse. If records of past use can be stored and reviewed upon an allegation of improper access or use, state and local educational agencies will be able to provide remedies for informational harm.

Our first recommendation is that internal use be tracked. We would suggest implementing a technological mechanism that would create audit trails for each user, storing both when they accessed the database and what information was reviewed. Such trails will allow administrators to more easily detect improper access.

Second, we would recommend maintaining records of all third party use of student data. State and local educational agencies should have clear procedures in place for third parties to apply for permission to access information. Records should be kept of the application and review process and, if access is granted, the release of information and eventual deletion of such information in compliance with FERPA following the completion of the permitted use.

Recommendation 7 – States should provide public notice and user friendly systems. The policies and procedures regarding the longitudinal database should be easy for parents and students to find, understand, and use. We would recommend an easy to navigate website that provides all necessary information about information collection and use. At a minimum the website should include the following: (i) an easy to read summary of the collection system, including how it works; (ii) a privacy policy explaining the rights of parents and students and how those rights are protected at the local and state levels; (iii) a copy of the data dictionary so that parents are aware of exactly what information is collected; (iv) an electronic record review and change procedure so that parents can easily stay up-to-date on what information is in their child's record; and (v) a clearly stated policy about third party use of the information and details on the application process for such use.

Recommendation 8- States should appoint a Chief Privacy Officer within the state's Department of Education to assure the respect for children's privacy in educational records and to oversee compliance with federal and state privacy laws. We strongly recommend the appointment of a Chief Privacy Officer in each state's department of education to assure the protection of children's privacy in state database programs. The Chief Privacy Officer should have the authority and responsibility to review and approve programs, proposals, and contracts with respect to their impact on privacy and compliance with existing legal privacy obligations. To accomplish these tasks, the Chief Privacy Officer should be charged with preparing and making publicly available a Privacy Impact Assessment for each state program, proposal, and vendor contract associated with statewide longitudinal databases of educational records. This will enable states to comply more effectively with their FERPA obligations and to assure more effectively that children's privacy is protected. Indeed, many of the privacy weaknesses and compliance failures at the state level could be avoided if a Chief Privacy Officer were in place.

B. Legislative Reform

In this section we provide some recommendations for legislative reform. While the recommended best practices are good practical guidance for those entities and institutions responsible for implementing the longitudinal databases, they do not create the level of accountability that can be obtained with regulation. Because we are concerned about children as a vulnerable population, we would recommend that critical privacy protections be required by statute or regulation. FERPA sets forth broad guidelines and restrictions, but the recent development of longitudinal databases has highlighted a number of more specific privacy protections that we believe should be mandatory.

First, we would recommend that the permissible reasons for data collection be more clearly defined. Specifically, we would suggest that state departments of education be required to articulate justifications for their collection of information. Under FERPA, state departments of education may simply indicate that information collection is necessary for "audit and evaluation," and we would suggest that they should be required to articulate why specific types of information aid an audit or evaluation. Such a requirement would help to limit the excessive data collection that we identified in states such as Florida, New Jersey, and Louisiana. One of the best ways to ensure states are acting in good faith is to require that they articulate their legitimate uses.

Second, we would recommend specific data retention limitations. FERPA currently requires under both the audit and evaluation exception and the research use exception that disclosed information should be deleted when the audit or research purpose is concluded. This general requirement, however, provides state departments of education and third parties with broad leeway. Arguably, a state could take the position that it needs to hold information indefinitely in order to monitor academic changes over time. We believe this vague standard allows too much flexibility and would recommend that state legislatures provide well defined time limits on data retention. Legislatures should investigate what type of evaluation is most valuable, the information required for such evaluation, and the risks of lengthy retention, and then set appropriate caps on data retention time. We would suggest that time periods in excess of five years are unnecessary and overly risky.

Lastly, we would recommend that an oversight mechanism for privacy at the state level be mandatory in connection with the collection and use of children's educational data. To this end, we recommend the statutory creation of a Chief Privacy Officer at the state department of education. The Chief Privacy Officer should have the authority and responsibility to review and approve programs, proposals, and contracts with respect to their impact on privacy and compliance with existing privacy law and should be required to report privacy impact assessments to the public. This institutional mechanism would serve a critical oversight need.

V. CONCLUSION

Data collection is on the rise in the K-12 educational systems across the nation, as well as in post-secondary educational systems. This trend is likely to continue in the future. While there are certainly some strong reasons for data collection, such as improving teaching methods and tracking school improvement, it is important to recognize the privacy risks inherent in these data collection systems. Our goal has been to identify privacy risks in the existing state systems as currently deployed and to provide some suggestions on how these problems can be addressed. Implementing best practices for privacy protection while these projects are still developing will help to create a foundation for privacy protections that can be built upon as collection continues.

APPENDIX A
Table of Directory Information

State	Name	Address	Date of Birth	Home School	Attending School	Enrollment Type	Entry Date	Exit Date	County of Birth	Country of Birth
AL†										
AK	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
AZ	Y				Y	Y			Y	Y
AR†										
CA	Y	Y	Y		Y	Y	Y	Y	Y	Y
CO	Y	Y	Y	Y	Y	Y				
CT*	Y	Y	Y	Y	Y					
DE*										
FL	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
GA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
HI*										
ID†										
IL	Y		Y	Y	Y	Y	Y	Y	Y	Y
IN*										
IA	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
KS	Y	Y	Y	Y	Y		Y	Y		
KY	Y	Y	Y			Y	Y	Y		Y
LA	Y	Y	Y	Y	Y		Y	Y		Y
ME	Y	Y	Y						Y	Y
MD†										
MA	Y	Y	Y		Y	Y	Y	Y	Y	Y
MI	Y	Y	Y	Y	Y		Y	Y	Y	Y
MN	Y		Y	Y	Y		Y	Y		
MS‡	Y	Y	Y				Y	Y	Y	Y
MO	Y		Y	Y	Y	Y				
MT	Y		Y				Y	Y		
NE	Y		Y	Y	Y		Y	Y		
NV†										
NH	Y		Y	Y	Y	Y	Y	Y	Y	
NJ	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
NM	Y		Y		Y	Y				
NY	Y	Y	Y	Y	Y		Y	Y	Y	Y
NC	Y	Y	Y		Y		Y	Y		Y
ND	Y	Y	Y	Y	Y	Y				Y
OH	Y		Y	Y		Y		Y	Y	
OK‡										
OR	Y		Y		Y			Y		
PA	Y		Y	Y	Y	Y	Y	Y	Y	Y
RI	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SC*	Y		Y			Y	Y	Y		
SD	Y		Y	Y	Y	Y	Y	Y		
TN	Y		Y	Y	Y	Y	Y	Y		
TX	Y		Y	Y	Y	Y		Y		
UT†										
VA	Y	Y	Y		Y	Y	Y	Y		Y
VT	Y		Y	Y	Y	Y		Y		
WA	Y	Y	Y	Y	Y	Y	Y	Y		Y
WV†										

WI	Y		Y	Y	Y		Y	Y		Y
WY	Y		Y	Y	Y		Y	Y		

† Indicates a state that may have a longitudinal database, but detailed information was not publicly available.
* Indicates a state database that is still in the development phase.
‡ Indicates a state that does have a longitudinal database, but we were unable to find a data dictionary.

APPENDIX B
Table of Personal Identifiers

State	Personal ID #	Social Security Number
AL†		
AK	Y	Y
AZ	Y	
AR†		
CA	Y	
CO	Y	
CT*	Y	
DE*	Y	
FL	Y	Y
GA	Y – Either SS# or Personal ID used	Y – Either SS# or Personal ID used
HI*		
ID†		
IL	Y	
IN*		
IA	Y	Optional
KS	Y	Optional
KY	Y	Y
LA	Y (usually SS#)	Y
ME	Y	
MD†		
MA	Y	
MI	Y	
MN		Y
MS‡		
MO	Y	Y
MT	Y	
NE	Y	
NV†		
NH	Y	
NJ	Y	
NM	Y	
NY	Y	
NC	Y	Optional
ND		
OH	Y	
OK‡		
OR		Y
PA	Y	Y
RI	Y	
SC*	Y	Y
SD	Y	Y
TN	Y	Y
TX	Y	
UT†		
VA	Y	
VT	Y	
WA	Y	Optional
WV†		

WI	Y	
WY	Y	

† Indicates a state that may have a longitudinal database, but detailed information was not publicly available.
* Indicates a state database that is still in the development phase.
‡ Indicates a state that does have a longitudinal database, but we were unable to find a data dictionary.

APPENDIX C
Table of Demographic Information

State	Gender	Race	Ethnicity	Immigration Status	LEP Status	Native Language	Migrant Status	Single Parent
AL†								
AK	Y	Y	Y	Y	Y	Y	Y	Y
AZ	Y	Y	Y	Y	Y	Y	Y	
AR†								
CA	Y	Y	Y		Y	Y	Y	
CO	Y		Y	Y	Y	Y	Y	
CT*	Y	Y	Y			Y	Y	
DE*								
FL	Y	Y	Y	Y	Y	Y	Y	Y
GA	Y	Y	Y	Y	Y	Y	Y	Y
HI*								
ID†								
IL	Y	Y	Y	Y	Y	Y	Y	
IN*								
IA	Y	Y	Y	Y	Y	Y	Y	
KS	Y	Y	Y	Y	Y	Y	Y	
KY	Y	Y		Y	Y	Y	Y	
LA	Y		Y	Y	Y	Y		
ME	Y	Y	Y	Y	Y	Y	Y	
MD†								
MA	Y	Y	Y		Y	Y		
MI	Y	Y	Y		Y	Y	Y	
MN	Y	Y	Y		Y	Y	Y	
MS‡								
MO	Y	Y	Y		Y		Y	
MT	Y	Y	Y	Y	Y	Y		Y
NE	Y	Y	Y	Y	Y	Y	Y	Y
NV†								
NH	Y	Y	Y		Y		Y	
NJ	Y	Y	Y		Y		Y	
NM	Y	Y	Y		Y	Y		Y
NY	Y	Y	Y	Y	Y	Y	Y	Y
NC	Y	Y	Y	Y	Y	Y	Y	
ND	Y	Y	Y	Y	Y		Y	
OH	Y	Y	Y		Y	Y	Y	
OK‡	Y	Y			Y		Y	
OR	Y		Y		Y			Y
PA	Y	Y	Y	Y	Y	Y	Y	Y
RI	Y	Y	Y	Y	Y	Y		Y
SC*	Y	Y	Y	Y	Y	Y	Y	
SD	Y	Y	Y	Y	Y	Y	Y	
TN	Y	Y	Y	Y		Y		
TX	Y		Y	Y	Y	Y	Y	
UT†								
VA	Y	Y	Y	Y	Y	Y	Y	
VT	Y	Y	Y					
WA	Y	Y	Y		Y	Y	Y	
WV†								

WI	Y	Y	Y	Y	Y	Y	Y	
WY	Y	Y	Y	Y			Y	

† Indicates a state that may have a longitudinal database, but detailed information was not publicly available.
* Indicates a state database that is still in the development phase.
‡ Indicates a state that does have a longitudinal database, but we were unable to find a data dictionary.

APPENDIX D
Table of Academic Information

State	Standardized Test Scores	Special Ed Status	Sec. 504 Testing Accommodation	Extra/ Tutoring Services	Gifted/ Talented	Post-Grad Plans	AP Courses	ACT & SAT Scores
AL†								
AK	Y	Y	Y	Y		Y		
AZ	Y	Y	Y	Y	Y			
AR†								
CA	Y	Y			Y			
CO	Y	Y	Y	Y	Y		Y	Y
CT*	Y							Y
DE*	Y							
FL	Y	Y	Y	Y	Y	Y		
GA	Y	Y^	Y	Y	Y			
HI*								
ID†								
IL	Y[367]		Y	Y				
IN*								
IA	Y		Y	Y	Y	Y		Y
KS	Y	Y		Y	Y	Y		
KY	Y	Y^		Y	Y	Y	Y	
LA	Y	Y						
ME	Y	Y	Y					
MD†								
MA	Y	Y				Y	Y	
MI	Y	Y					Y	
MN	Y	Y		Y	Y			
MS‡	Y							
MO	Y	Y^			Y	Y		
MT	Y	Y	Y	Y	Y	Y		
NE	Y	Y	Y		Y			
NV†								
NH	Y	Y	Y	Y		Y	Y	
NJ	Y	Y^						
NM	Y	Y^		Y		Y		
NY	Y	Y	Y			Y		
NC	Y	Y			Y			
ND	Y	Y	Y					
OH	Y	Y	Y		Y		Y	
OK‡	Y	Y		Y				
OR	Y	Y			Y			
PA	Y	Y	Y		Y	Y		
RI	Y	Y				Y		
SC*	Y	Y						
SD	Y	Y						
TN	Y							
TX	Y	Y			Y	Y		

[367] Includes reasons for not testing. Codes include: jail, homebound exempt and medically exempt.

^ Includes type of disability

UT†								
VA	Y	Y		Y	Y	Y	Y	
VT	Y		Y					
WA	Y	Y^	Y		Y		Y	
WV†								
WI	Y		Y					
WY	Y		Y		Y			

† Indicates a state that may have a longitudinal database, but detailed information was not publicly available.
* Indicates a state database that is still in the development phase.
‡ Indicates a state that does have a longitudinal database, but we were unable to find a data dictionary.

APPENDIX E
Table of Disciplinary Information

State	Withdraw Reason	Coded Reasons Includes: Jail, Illness, Drop Out, or Mental Health	Disciplinary Action Date	Disciplinary Reason	Weapon Type	# of Absences	# of Suspensions
AL†							
AK	Y	Y	Y	Y	Y	Y	Y
AZ	Y	Y[368]				Y	
AR†							
CA	Y	Y	Y				
CO							
CT*			Y	Y			
DE*							
FL	Y	Y	Y	Y[369]	Y	Y	Y
GA	Y	Y[370]	Y	Y	Y	Y	Y
HI*							
ID†							
IL	Y		Y	Y			
IN*							
IA	Y	Y	Y	Y	Y	Y	
KS	Y	Y				Y	
KY	Y		Y	Y		Y	
LA	Y	Y[371]	Y	Y	Y	Y	
ME							
MD†							
MA							Y
MI	Y	Y	Y	Y	Y	Y	
MN	Y	Y					
MS‡							
MO	Y	Y	Y	Y	Y		Y
MT	Y	Y				Y	
NE						Y	
NV†							
NH	Y	Y				Y	Y
NJ	Y	Y					
NM	Y	Y		Y	Y		
NY							
NC	Y	Y	Y	Y	Y	Y	Y
ND	Y					Y	
OH	Y	Y	Y	Y		Y	
OK‡							
OR	Y						
PA	Y	Y[372]				Y	
RI	Y	Y	Y	Y	Y	Y	
SC*	Y						

[368] Reasons also include pregnancy and victim of a crime.

[369] Coded reasons include hate crimes and gang-related violence.

[370] Reasons also include pregnancy and financial hardship.

[371] Reasons also include pregnancy.

[372] Reasons also include pregnancy.

SD	Y	Y				Y	
TN	Y	Y	Y	Y	Y	Y	
TX	Y			Y		Y	
UT†							
VA	Y	Y				Y	
VT	Y						
WA	Y	Y[373]				Y	
WV†							
WI	Y		Y	Y			
WY							

† Indicates a state that may have a longitudinal database, but detailed information was not publicly available.
* Indicates a state database that is still in the development phase.
‡ Indicates a state that does have a longitudinal database, but we were unable to find a data dictionary.

[373] Reasons also include pregnancy.

APPENDIX F
Table of Economic Information

State	Free/ Reduced Lunch	Homeless Status	Homeless Living Place
AL†			
AK		Y	Y
AZ	Y	Y	
AR†			
CA	Y		
CO	Y	Y	Y
CT*	Y	Y	
DE*			
FL	Y	Y	Y
GA	Y	Y	Y
HI*			
ID†			
IL	Y	Y	
IN*			
IA	Y	Y	
KS	Y		Y
KY	Y	Y	Y
LA	Y	Y	Y
ME	Y	Y	
MD†			
MA			
MI	Y	Y	Y
MN	Y	Y	
MS‡			
MO	Y	Y	Y
MT	Y	Y	Y
NE	Y	Y	Y
NV†			
NH	Y	Y	Y
NJ	Y		
NM	Y	Y	
NY	Y	Y	Y
NC	Y	Y	
ND	Y		
OH	Y	Y	Y
OK‡	Y		
OR	Y		
PA	Y	Y	
RI	Y	Y	
SC*	Y	Y	
SD	Y	Y	Y
TN			
TX			
UT†			
VA		Y	
VT	Y		
WA	Y	Y	

WV†			
WI		Y	
WY	Y	Y	

† Indicates a state that may have a longitudinal database, but detailed information was not publicly available.

* Indicates a state database that is still in the development phase.

‡ Indicates a state that does have a longitudinal database, but we were unable to find a data dictionary.

APPENDIX G
Table of Health-Related Info

State	Insurance Status	Medicaid Number	Date of Last Medical Exam	Date of Last Lead Test	Lead Level	Immunization Status
AL†						
AK						
AZ						
AR†						
CA						
CO						
CT*						
DE*						
FL			Y			Y
GA						
HI*						
ID†						
IL						
IN*						
IA						
KS						
KY			Y			Y
LA						
ME		Y				
MD†						
MA						
MI						
MN						
MS‡						
MO						
MT						
NE						
NV†						
NH						
NJ	Y		Y	Y	Y	Y
NM						
NY						Y
NC	Y	Y	Y			
ND						
OH						
OK†‡						
OR						
PA						
RI		Y				
SC*		Y				
SD						
TN						
TX						
UT†						
VA						
VT						
WA†						

WV†						
WI						
WY						

† Indicates a state that may have a longitudinal database, but detailed information was not publicly available.
* Indicates a state database that is still in the development phase.
‡ Indicates a state that does have a longitudinal database, but we were unable to find a data dictionary.

APPENDIX H

Bibliography of State Materials

Set forth below is a list of the most substantial state reference materials we collected and used in the preparation of this report. All URLs were last visited on February 18, 2009.

State	Materials
AL†	
AK	Alaska Student ID System Information Brochure, *available at* http://www.eed.state.ak.us/oasis/asidsbrochure.pdf. Design Document for the Alaska Student ID System (Revision 1.04b), *available at* http://www.eed.state.ak.us/oasis/alaskadesigndocument.pdf.
AZ	Code Values (Version 4.8), *available at* http://azed.gov/sais/codevalues/DataTransactionCodeValues.pdf. FY 2009 – SAIS Changes Overview, *available at* http://www.azed.gov/sais/Downloads/FY-09_SAIS_Overview.pdf. SAIS Data Retention Guidelines, *available at* http://www.azed.gov/sais/downloads/SAISDataRetentionGuidelines.doc. ARIZ. REV. STAT. ANN. § 15-1042 (2009), *available at* http://www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/15/01042.htm&Title=15&DocType=ARS.
AR†	
CA	California School Information Services, http://www.cde.ca.gov/ds/sd/cs/. California Longitudinal Pupil Achievement Data System, http://www.cde.ca.gov/ds/sp/cl/index.asp. CSIS Frequently Asked Questions about Statewide Student Identifiers, http://www.csis.k12.ca.us/faq/si-faq.asp. Statewide Student Identifier User Guide (Version 2.2), *available at* http://www.csis.k12.ca.us/library/statewide-identifier/SSID-User-Guide-for-SB1453-v2-2-20080929.pdf.
CO	Student Identifier Management Unit Index, http://www.cde.state.co.us/cdesim/index.htm. RITS Web Application User Guide (Version 1.2), *available at* http://www.cde.state.co.us/cdesim/downloads/pdf/RITSUserGuide.pdf. RITS Web Application School User Packet (Version 1.4), *available at* http://www.cde.state.co.us/cdesim/downloads/pdf/RITSUserPacket.pdf.

CT*	Project Abstract, http://www.csde.state.ct.us/public/cedar/slds/data_dictionary.htm.
DE*	
FL	Data Elements and Definitions, http://edwapp.doe.state.fl.us/bsn_subjects/SubjectsFacetsList.aspx. Education Data Warehouse – Functional Rules (Version 5.1), *available at* http://edwapp.doe.state.fl.us/Documents/functional_spec.pdf. Student & Public Records: An Overview of Legal Issues (June 19, 2008) (on file with author). Education Records of Pupils and Adult Students, FLA. ADMIN. CODE ANN. R. 6A-1.0955 (2008), *available at* http://www.doh.state.fl.us/Family/School/legislative/6A-10955.pdf.
GA	
HI*	IT Projects – Milestones, http://doe.k12.hi.us/technology/projects/milestones.htm (referencing the development of the student database eSIS).
ID†	Idaho State Department of Education—Data Collection, http://www.sde.idaho.gov/site/data_collection.htm.
IL	ISBE Student Information Systems User Manual, *available at* http://www.isbe.state.il.us/sis/html/user_manual.htm (follow the link to download the manual as a pdf or word document). ISBE SIS Data Elements, *available at* http://www.isbe.state.il.us/sis/html/data_elements.htm (follow the links to download pdf versions of the various data elements). ISBE SIS Frequently Asked Questions, *available at* http://www.isbe.state.il.us/sis/pdf/qa_20060525.pdf Contractual Agreement by and between the Illinois State Board of Education and International Business Machines (on file with author).
IN*	
IA	Project EASIER — Iowa Department of Education, http://www.iowa.gov/educate/index.php?option=com_content&task=view&id=44&Itemid=12 (follow the links to download the Data Dictionary 2008-2009 (Version 2009.1)). Project EASIER Supplement, Sept. 2007, *available at* http://www.iowa.gov/educate/index.php?option=com_docman&task=doc_download&gid=3998. Downloads – State ID – Data Collections – Iowa Department of Education,, http://www.iowa.gov/educate/index.php?option=com_docman&task=cat_view&gid=321&Itemid=1563 (follow the links to download State ID User Manuals and Policy

	Statements). Project EASIER, 2007-2008 Fall Data Reporting Requirements, *available at* http://www.iowa.gov/educate/index.php?option=com_docman&task=doc_download&gid=4465. Fall 2008 Checklist, *available at* http://www.iowa.gov/educate/index.php?option=com_docman&task=doc_download&gid=5707. EdInsight – Data Warehouse – Iowa Department of Education, http://www.iowa.gov/educate/index.php?option=com_content&task=view&id=1691&Itemid=2490
KS	KIDS 2008-2009 Collection System File Specifications, *available at* http://www.ksde.org/LinkClick.aspx?fileticket=CfXC6hszkis%3d&tabid=2508&mid=6013. KIDS Collection Field Requirement by Record Type, *available at* http://www.ksde.org/LinkClick.aspx?fileticket=RnEl1Sl%2biXA%3d&tabid=2508&mid=6013. KIDS 2008-2009 User Guide, *available at* http://www.ksde.org/LinkClick.aspx?fileticket=J2w5%2bp5dWfY%3d&tabid=2508&mid=6013. KSDE Data Access and Use Policy, *available at* http://www.ksde.org/LinkClick.aspx?fileticket=ndfZ%2bqai7vQ%3d&tabid=2508&mid=6013. SIS Vendor Info, http://www.ksde.org/Default.aspx?tabid=2516. Answers to Parents' Questions (Apr. 2005) (on file with author). Kansas Application for Grants, *available at* http://nces.ed.gov/Programs/SLDS/pdf/Kansas.pdf.
KY	2008-2009 Final Data Standards, *available at* http://education.ky.gov/NR/rdonlyres/E74F4406-2806-4362-BEFD-D489D32B0BDB/0/200809_DataStandards11708FINAL2.pdf. STIHealth v. 11 Data Standards, *available at* http://education.ky.gov/NR/rdonlyres/1C57DCBC-2320-43AD-859C-0ED359232413/0/STIHealthStandardsV11.pdf. New Student Information System Initiative—About the Infinite Campus SIS Initiative, http://education.ky.gov/KDE/Administrative+Resources/Data+and+Research/Student+Information+System/New+Student+Information+System+Initiative/. Agreement by and between Kentucky Department of Education and Infinite Campus,

	dated Nov. 20, 2006. Agreement by and between Kentucky Department of Education and Claraview, Inc., dated June 1, 2007.
LA	SIS User Guide (ver. 8.6), *available at* http://www.doe.state.la.us/lde/uploads/7706.pdf. STS User Guide 2008-2009, *available at* http://www.doe.state.la.us/lde/uploads/1337.pdf. SER User Guide, *available at* http://www.doe.state.la.us/lde/uploads/11236.pdf. Guidance for the Family Educational Rights and Privacy Act, *available at* http://www.doe.state.la.us/lde/uploads/3312.pdf. Security and Confidentiality Statement for the LEAPweb Reporting System, *available at* https://www.leapweb.org/LEAPweb_system_oath_form.pdf. Louisiana Educational Accountability Data System 2007-2008 LEADS User Guide Draft (on file with author).
ME	MEDMS On-line User Manual, https://www.medms.maine.gov/MEDMS/usermanual/unit1.htm. Agreement to Purchase Services, by and between the State of Maine, Department of Education and Xwave New England Corp., dated Mar. 13, 2003 (on file with author).
MD†	
MA	SIMS Version 2.1 Data Handbook, *available at* http://www.doe.mass.edu/infoservices/data/sims/DataHandbook.doc. SIMS User Guide Version 2.0, *available at* http://www.doe.mass.edu/infoservices/data/sims/UserGuide.doc. Introduction to SIMS, *available at* http://www.doe.mass.edu/infoservices/data/sims/intro_sims.pdf.
MI	Michigan Education Information System Single Record Student Database Data Field Description (Spring/End of Year 2008), *available at* http://www.michigan.gov/documents/cepi/spr2009_SRSD_field_descriptions_258932_7.pdf. New to SRDS? Information Packet, *available at* http://www.michigan.gov/documents/NewToSRSD1004_106632_7.pdf. CEP—SRSD/UIC Security Agreements, http://www.michigan.gov/cepi/0,1607,7-113-986_10481-3831--,00.html.
MN	MARSS Manual, *available at* http://education.state.mn.us/mdeprod/groups/Finance/documents/Manual/002857.pdf.

	Data Element Definitions, *available at* http://education.state.mn.us/MDE/Accountability_Programs/Program_Finance/MARSS_Student_Accounting/MARSS_Instruction_Manual/Data_Elements-Definitions/index.html (offering downloadable versions of each element and the entire data dictionary). List of Software Vendors Certified for Reporting, http://education.state.mn.us/MDE/Accountability_Programs/Program_Finance/MARSS_Student_Accounting/index.html.
MS‡	MSIS 1 and 2 - Oath of Confidentiality, *available at* http://www.mde.k12.ms.us/msis/documents/msis_sec_022006.pdf. MSIS 4 – Oath of Confidentiality, *available at* http://www.mde.k12.ms.us/msis/documents/updated_msis_mde_sec_012009.pdf. MSIS Frequently Asked Questions, http://www.mde.k12.ms.us/msis/faq.html. The History of MSIS, http://www.mde.k12.ms.us/msis/history.html.
MO	Core Data Collection System Manual (ver. 19), *available at* http://dese.mo.gov/divimprove/coredata/Manual%202008.doc. MOSIS Code Sets (July 24, 2008), http://dese.mo.gov/MOSIS/CodeSetExcelDocument.html#Discipline_Removal_Codes. MOSIS Project Overview, http://dese.mo.gov/MOSIS/overview.html.
MT	Achievement in Montana Data Dictionary (ver. 2008.2.5), *available at* http://opi.mt.gov/Pub/AIM/DTA%20Dictionary/AIM%20Data%20Dictionary%20v1.08.pdf. Student Records Confidentiality Policy, (Feb. 1, 2008), *available at* http://opi.mt.gov/pub/AIM/AIM%20Policies/Student_record_confidentiality%20Policy.pdf. MONT.CODE. ANN. § 20-2-212 (2007). 2MONT.CODE. ANN. § 20-1-213 (2007). Montana Local Government Retention and Disposition Schedules X, XIII (on file with author). Contract for Achievement in Montana, by and between State of Montana, Montana Office of Public Instruction and Infinite Campus, as amended (on file with author).
NE	Student Template Instruction Manual, *available at* http://www.nde.state.ne.us/nssrs/Docs/STUDENT_MANUAL_3_0_0.pdf.

	Assessment Template Instruction Manual, *available at* http://www.nde.state.ne.us/nssrs/Docs/ASSESSMENT_MANUAL_3_0_0.pdf. Title I Programs Template Instruction Manual, *available at* http://www.nde.state.ne.us/nssrs/Docs/TITLE_I_PROGRAMS_MANUAL_3_0_0.pdf. Programs Fact Template Instruction Manual, *available at* http://www.nde.state.ne.us/nssrs/Docs/PROGRAMS_FACT_MANUAL_3_0_0.pdf. NSSRS Uniq-Id Step-by-Step Guide, *available at* http://www.nde.state.ne.us/nssrs/Docs/NSSRS_Steps_Uniqid.pdf. Nebraska Data Access and Management Policy, *available at* http://www.nde.state.ne.us/nssrs/Docs/NE_Data_Access_and_Management_Policy505.doc.
NV†	
NH	Data Dictionary, https://ww4.ed.state.nh.us/datadictionary/. Policy and Procedures Manual for i4see and Related Data, *available at* http://www.ed.state.nh.us/education/datacollection/i4see/NH%20i4see%20Policy%20Manual%20v080220.doc. A Guide to How Data Improves Student Achievement, *available at* http://www.ed.state.nh.us/education/News/DataInitiativeFactSheet.pdf.
NJ	NJ SMART Background, http://www.state.nj.us/education/njsmart/background/. Student Data Handbook, *available at* http://www.state.nj.us/education/njsmart/download/SIDManagementStudentDataHandbook.pdf. Special Education Student Data Handbook, *available at* http://www.state.nj.us/education/njsmart/download/SpecialEducationStudentDataHandbook.pdf. State Submission Student Data Handbook, *available at* http://www.state.nj.us/education/njsmart/download/StateSubmissionStudentDataHandbook.pdf. Official Communications regarding NJ SMART, *available at* http://www.state.nj.us/education/njsmart/download/ (follow the links to find the official communications). Agreement by and between Public Consulting Group and the New Jersey Division of Purchase and Property, on behalf of the Department of Treasury and the Department of Education, as amended (on file with author).
NM	Student Identification System Application User Guide (ver. 5.0), *available at*

	http://www.ped.state.nm.us/stars/documents/User_Guide_v5.0.pdf. STARS Manual Volume 1 – User Guide, *available at* http://www.ped.state.nm.us/stars/dl09/SY2009%20STARS%20MANUAL-VOLUME%201.pdf. STARS Manual Volume 2 – Reference Materials, *available at* http://www.ped.state.nm.us/stars/dl09/SY2009%20STARS%20MANUAL-VOLUME%202.pdf. STARS User Authorization Form, *available at* http://www.ped.state.nm.us/stars/documents/STARS_Username_Form_3.pdf.
NY	SIRS Policy Manual (ver. 3.1) (on file with author). SIRS Dictionary of Reporting Data Elements (ver. 3.1) (on file with author). SIRS Users Guide (ver. 5.4) (on file with author). The above mentioned documents are now combined into one guidebook, *available at* http://www.emsc.nysed.gov/irts/SIRS/2008-09/2008-09SIRS-MANUAL-4-1.pdf.
NC	Training eSIS Documents Home, http://www.ncwise.org/TRAINING/ncwise_training_documents/training_pg_esis_home.html (collecting NC WISE eSIS Data Element Definitions). What's NC WISE, *available at* http://www.ncwise.org/documents/ncwise/What_Is_NC%20WISE.pdf. Introduction to Student Demographics (last updated Nov. 20, 2007) (on file with author).
ND	STARS User Manual, http://www.dpi.state.nd.us/resource/STARS/Reports/manual.shtm. Data Dictionary, http://www.dpi.state.nd.us/resource/STARS/layouts/index.shtm. Online Reporting System General Information, http://www.dpi.state.nd.us/resource/ORS/general/index.shtm. N.D. CENT. CODE § 15-10-17 (2007), *available at* http://www.legis.nd.gov/cencode/t15c10.pdf.
OH	ODE—2008 EMIS Manual, http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEDetail.aspx?page=3&TopicRelationID=1102&ContentID=25338&Content=60675. ODE—EMIS Handbook, http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEDetail.aspx?page=3&TopicRelationID=367&ContentID=38908&Content=60686 (follow the links to EMIS handbooks for 2008 and 2009).

	ODE—Statewide Student Identifier Manuals, http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEDetail.aspx?page=3&TopicRelationID=1102&ContentID=11215&Content=60670. ODE—Presentations—EMIS, http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEDetail.aspx?page=3&TopicRelationID=1577&ContentID=23201&Content=61537. ODE—2003 EMIS Manual, http://www.ode.state.oh.us/GD/Templates/Pages/ODE/ODEDetail.aspx?page=3&TopicRelationID=1101&ContentID=12084&Content=50921. Ohio SLDS Application Profile, *available at* http://nces.ed.gov/Programs/SLDS/pdf/Ohio.pdf.
OK‡	Press Release, CPSI Ltd., Oklahoma Deploys the Nation's First Fully Implemented Statewide SIF-Based Data Collection Model (Aug. 8, 2005), *available at* http://vcasel.com/Company/NewsReleases/tabid/116/Default.aspx. 70 OKLA. STAT. tit. 70, § 3-161 (2007), *available at* http://webserver1.lsb.state.ok.us/OK_Statutes/CompleteTitles/os70.rtf (Student Tracking and Reporting (STAR) Pilot Program).
OR	Data Dictionary, http://www.ode.state.or.us/data/kids/datadictionary/. Data Project Governance Plan (ver. 1.1), *available at* http://www.oregondataproject.org/system/files/DATAProject_GovernancePlan_v1.1.pdf. Progress Reviews—The Oregon DATA Project, http://www.oregondataproject.org/content/progress-reviews. Data Project Overview, *available at* http://www.oregondataproject.org/system/files/DATAProjectOverview_2209-0123.ppt#256,1,Slide 1.
PA	PIMS User Manual Volume 1, *available at* http://www.edportal.ed.state.pa.us/portal/server.pt/gateway/PTARGS_0_2_319297_0_0_18/PIMS%20Manual%20-%20Volume%201_v1.7.1.pdf. PIMS User Manual Volume 2, *available at* http://www.edportal.ed.state.pa.us/portal/server.pt/gateway/PTARGS_0_2_319298_0_0_18/PIMS%20Manual%20-%20Volume%202_v1.7.1.pdf. Student Data Access and Use Policy, *available at* http://www.edportal.ed.state.pa.us/portal/server.pt/gateway/PTARGS_0_2_335984_0_0_18/PDE_Data_Access_Policy.pdf. PIMS Voluntary Vendor Participation Program, http://www.edportal.ed.state.pa.us/portal/server.pt?open=512&objID=1839&&PageID=299313&level=2&css=L2&mode=2&in_hi_userid=2&cached=true.

RI	Common Core Data Elements, https://www.eride.ri.gov/dataElements/CCDataBook.asp (state data dictionary). RIDE Data Warehouse, http://www.ride.ri.gov/onis/DW/DataWarehouse.aspx.
SC*	Data Collection Manual (2007-2008), *available at* http://ed.sc.gov/agency/Accountability/Technology-Services/old/dts/documents/07-08datacollectionmanual.doc. Data Collection Spreadsheet, *available at* http://ed.sc.gov/agency/Accountability/Technology-Services/old/dts/documents/datacollectionspreadsheet_001.xls. Data Access and Management Policy, *available at* http://ed.sc.gov/agency/Accountability/Technology-Services/Documents/5-3DraftDataAccessPolicy.pdf. SASI Data Guidelines, *available at* http://ed.sc.gov/agency/Accountability/Technology-Services/Documents/5-3SASIDataGuidelines.pdf. SUNS District User Guide, *available at* http://ed.sc.gov/agency/Accountability/Technology-Services/Documents/SCSUNSDistrictUserGuide.pdf.
SD	List of Data Elements, *available at* http://doe.sd.gov/ofm/sims/pdf/Data%20Elements%202-2005.pdf. Special Education Data Elements, *available at* http://doe.sd.gov/oess/specialed/docs/SIMSManual8-08.pdf. South Dakota SIMS Net Instruction Manual (on file with author). Protecting the Privacy of Student Education Records, http://doe.sd.gov/ofm/sims/Privacy.asp. South Dakota Department of Education and Cultural Affairs, http://doe.sd.gov/ofm/sims/POLICY1.HTM (displaying a policy statement concerning student records – data confidentiality).
TN	TN Department of Education: K-12, http://www.tennessee.gov/education/eis/index.shtml (follow the links to download the Education Information System User Manual). Complete Data Dictionary, *available at* http://www.tennessee.gov/education/eis/doc/manual_dictionary.pdf. Data Dictionary, *available at* http://www.tennessee.gov/education/eis/doc/datadict01.pdf. Next Generation Data Collection Tools Logical Diagram, *available at*

	http://www.tennessee.gov/education/eis/doc/data_tools_diagram.pdf.
TX	TREx Data Standards (2008-2009), http://ritter.tea.state.tx.us/trex/datastds/datastds_08-09_33.html. Letter to the Administrator Addressed (Sept. 4, 2008), *available at* http://ritter.tea.state.tx.us/taa/comm090408.html. TEA—PEIMS Data Standards, http://ritter.tea.state.tx.us/peims/standards/index.html. PEIMS EDIT+ User Reference and Training Manual, *available at* http://ritter.tea.state.tx.us/peims/editplus/documents/RG_User09F.pdf. What is EDIT+?, http://ritter.tea.state.tx.us/peims/editplus/whatis.html. EDIT+ Frequently Asked Questions, http://ritter.tea.state.tx.us/peims/editplus/faq.html#GEN1.
UT†	
VA	Procedures for Data Collecting and Reporting, *available at* http://www.doe.virginia.gov/VDOE/Publications/ProceduresPDF.pdf. Education Information Management User Guide, *available at* https://p1pe.doe.virginia.gov/ssws/sswswebapp/jsp/common/SSWS_User_Guide.pdf. SRC Page, http://www.doe.virginia.gov/VDOE/Publications/student-coll/codes.html (follow the links to data codes and definitions). Data Elements for Student Record Collection, *available at* http://www.doe.virginia.gov/VDOE/Publications/student-coll/08-09/data-elements.pdf. Specifications for Collecting the Student Record Collection, *available at* http://www.doe.virginia.gov/VDOE/Publications/student-coll/08-09/specifications-document.pdf.
VT	Data Reporting Instructions, *available at* http://education.vermont.gov/new/pdfdoc/pgm_IT/collections/fall_census_09_report.pdf. Vermont Student Census – Online Software Instructions, *available at* http://education.vermont.gov/new/pdfdoc/pgm_IT/collections/fall_census_09_software.pdf. Collecting and Reporting Quality Data: The Best Practices Guide for Completing the Vermont Department of Education Core Data Collection, *available at* http://education.vermont.gov/new/pdfdoc/pgm_IT/training_materials/best_practices_guide.pdf.
WA†	Annual Data Collection Manual, *available at*

	http://www.k12.wa.us/DataAdmin/pubdocs/FormsSch/DataCollectionPln200809.pdf. CEDARS Data Manual, January 2009 – Version 2.0, *available at* http://www.k12.wa.us/DataAdmin/pubdocs/CEDARSDataManualv20January2009.doc.
WV†	
WI	Individual Student Enrollment System (ISES) User Manual, http://dpi.state.wi.us/lbstat/isesmanual.html. ISES CODES, http://dpi.state.wi.us/lbstat/isescodes.html (collecting ISES data codes and definitions). ISES Discipline Data Collection and Reporting, http://dpi.state.wi.us/lbstat/isesdiscip.html. ISES Guiding Principles, http://dpi.state.wi.us/lbstat/isesprinc.html. ESEA Report Card, http://dpi.state.wi.us/lbstat/isesfaq1.html. Wisconsin's Individual Student Enrollment System, http://dpi.state.wi.us/lbstat/isesfaq2.html. Protecting Student Privacy in Wisconsin, http://dpi.state.wi.us/lbstat/dataprivacy.html. Wisconsin Pupils Records Law 118.125 Pupils Records (on file with author).
WY	Data Elements and Rules, *available at* http://www.k12.wy.us/WISE/Documents/Library/DataElements/2008/WY-2008602_DataElementsAndRules-v0p5.pdf. Staffing Manual and Data Collection Guidebook, *available at* http://www.k12.wy.us/WISE/Documents/Library/TrainingMaterials/2008/Oct_2008_WDE602_DCG_and_Staff_Manual_09042008.pdf. Professional Service Contract for WSN, by and between the Wyoming Department of Education and ESP Solutions Group (on file with author). Professional Services Contract for WISE, by and between the Wyoming Department of Education and ESP Solutions Group (on file with author).

† Indicates a state that may have a longitudinal database, but detailed information was not publicly available.
* Indicates a state database that is still in the development phase.
‡ Indicates a state that does have a longitudinal database, but we were unable to find a data dictionary.