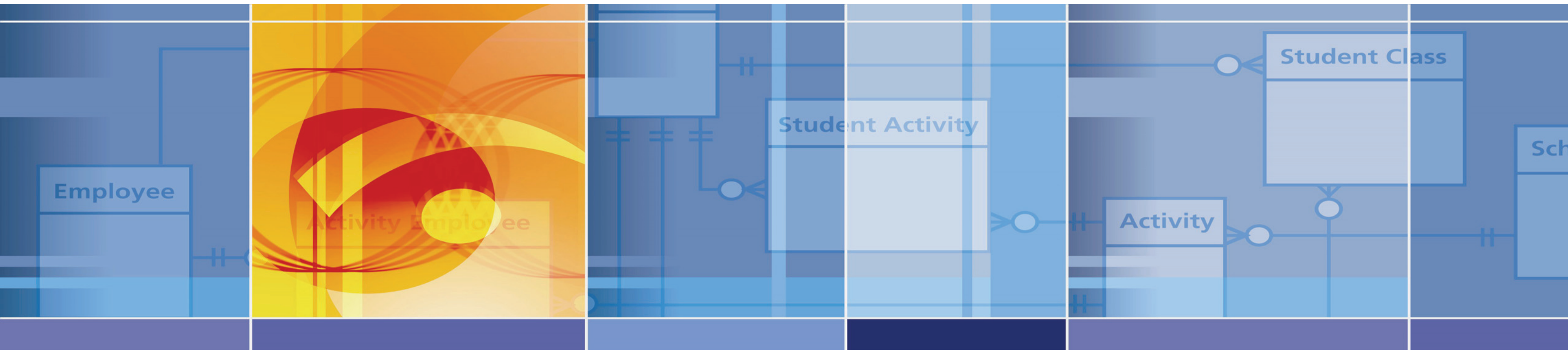


The Optimal Reference Guide:

Guidelines for Accessing Student Records in a State Longitudinal Database

Data Warehouse Series – Part III

Extraordinary insight into today's education topics

Barbara Clements, Ph.D., ESP Solutions Group
Greg Nadeau, ESP Solutions Group

With a foreword by Glynn D. Ligon, Ph.D., ESP Solutions Group

ESP Solutions Group

Table of Contents

Foreword 3

Laws Requiring Protection of Student Records 7

Longitudinal Student Records Systems 9

- Identifying Data for Inclusion in Longitudinal Student Records Systems 10
- Procedures for Secure Collection of Data 11
- Secure Maintenance of Student Data within the State Education Agency 11
- Determining Who Has Access to State Individual Student Records 11
- Levels of Access 15
- Providing Data from the Longitudinal Student Records System 18

General Recommendations for Protecting the Confidentiality of Education Records Maintained at the State Education Agency 19

Specific Recommendations 24

Summary 26

References 27

Foreword

By Glynn D. Ligon, Ph.D.

A few years ago, I was invited to volunteer to help the over-worked counselors at our local high school. They needed people to review graduation requirements and make sure individual students had met all requirements to graduate. My FERPA alarm went off right away, and I did what we dads do — donated money to the graduation party instead. This was in the same state where I was told I could not see my own actual score on the educator competency test for certification. This was the same district that had published the average test score for our son's grade level when there was only one other student who had voluntarily taken a test. This was all in the town where the university was hacked twice — once losing control of my Social Security Number and once of my daughter's. Actually, I could go on, because there were other incidents.

So I read this white paper with personal interest to see if there are any new solutions, any promise that personally identifiable information in our education information systems is going to be safer in the future than it has been. The bottom line? We must have clear and precise policies that direct agencies to follow clear and specific processes — no short cuts, no easy solutions, and no free pass on the almost impossible balance between easy access for authorized users and security. Whether access was ever an easy issue to monitor or not, it promises to continue to increase in complexity.

If "locks only keep honest people out," then are we just as misguided in how we restrict access to our useful education data? Are we so wary of unauthorized access to confidential information that we have designed elaborate systems that keep legitimate users out? Maybe we are not keeping them out physically, but the series of portals, sign-ons, and passwords between them and the data they need might be too much to navigate.

In 1996, I wrote a paper for the National Center for Education Statistics (NCES) on the future of education information systems, *New Developments in Technology: Implications for Collecting, Storing, Retrieving, and Disseminating National Data for Education.* One of my "predictions" was that dissemination would be replaced by access. So much effort was being put into disseminating copies of reports in 1996 that it was clear that we needed our future information systems to deliver to us just what we needed at the time we needed it. So here we are, a decade later and worried about managing access.

I am convinced that we are at a better place for data driven decision making (D3M). I encourage us all to open our information systems as much as possible to encourage use rather than be stymied by a fear that a few people might see some information they are not authorized to access. Our collective wisdom will keep us from erring too far on the side of openness. In the meantime, better informed decisions just might improve the teaching and learning process for our students.

When developing a longitudinal student records system at the state or local level, an important aspect to consider is who will have access to the information contained within the system, since the contents of student records are supposed to be zealously guarded according to the Family Educational Rights and Privacy Act (FERPA). This paper addresses the types of policies and procedures that are needed to ensure that access to student records is only available to persons with a "legitimate educational interest."

This document has been revised to reflect proposed revisions to FERPA regulations expected to be completed by summer 2008. Where specific guidance has been developed, clarification has been added to the text. However, there are issues covered in the revised regulations that do not relate directly to data maintained in state longitudinal student databases; these revisions and comments are not addressed in this paper.

When parents enroll their children in school, a **student record** is created. Parents provide certain types of information about the family (e.g., parents' names, home address, telephone number, sibling information), the child (e.g., date of birth, place of birth, home language, immunizations), and other areas of interest to the school (e.g., name of emergency contact). This information is entrusted to the school (and the district where the school is located) with the assumption that the information will be used only when necessary for ensuring that proper educational experiences and services are provided to the child.

While the child is in school, the student record is filled with information relating to the educational activities of the child, any services provided, and other aspects of the child's educational experience. Information about attendance, course completion and grades, honors, program participation, transportation, assessments, extracurricular activities, etc. is compiled in the record as milestones are met or as the need for a paper trail arises. Information is contributed by teachers, administrators, counselors, school health officials, program directors, and others within the education system. In rare instances, information about events from outside school hours and locales is entered into the student's record, such as information related to legal, health, or family problems. Clearly, there may be sensitive information in a student record that should be zealously guarded for the sake of the child.

When a child seeks to transfer to a school in another school district, the receiving school/district has a right to obtain a copy of the student's record. The receiving school/district can receive any information the sending school chooses to provide.

A subset of this information is included in the student's **transcript**. A transcript is typically sent to a postsecondary institution where a student is applying, to a scholarship organization, to the military, or to an employer if requested. It contains information about course completion and grades, honors, activities, and other information that is not quite as sensitive as other data maintained in the student record. The student (or his/her parent) gives permission for the transcript to be sent.

ESP Insight

Federal and State laws place restrictions on who has access to student records, but not the various types of data maintained within the record.

Federal and state laws place restrictions on who may have access to student records. These laws specify requirements that must be met by education agencies to guard the contents of the student records. These laws do not, however, restrict what data may be collected and maintained about students. That is left up to the educators who must decide whether specific data are needed to ensure appropriate educational and support services are provided to each student and whether the maintenance of the data is ethical. Schools and districts must decide what policies and procedures are needed to restrict who has access to the students' records.

Historically, student records have been maintained in a variety of places, mostly in paper files in filing cabinets in the school office or in teachers' classrooms. Attempts to merge the information for a student from various sources are often cumbersome and sometimes unsuccessful, such as when a student transfers from one school to another. Accumulating information across student groups for state and federal reporting is difficult and time-consuming. Security is virtually non-existent. Locked file cabinets in schools rarely stay locked during the day because information is needed from them. Still there have been few concerns about the confidentiality of the education records or about the misuse of information kept within them.

Computers have made it easier to keep larger amounts of information in one location (or linkable locations) and to use the information for making effective and efficient education decisions. But computerizing student records has raised a number of concerns about confidentiality and misuse of the information by persons who should not have access to the information in a student record. It is the responsibility of an education agency maintaining records about individual students to ensure that confidentiality and security concerns are addressed and that parents and students are informed of the measures used.

ESP Insight

It is the responsibility of an education agency maintaining records about individual students to ensure that confidentiality and security concerns are addressed and that parents and students are informed of the measures used.

The purpose of this paper is to provide guidance concerning the policies and procedures needed to ensure access to an electronic student record and its contents only by those who have a "legitimate educational interest." The paper contains information about:

- The role of federal and state laws restricting who may have access to a student record and its contents
- Longitudinal data systems and how they are maintained at the state and local levels
- Data elements and levels of sensitivity
- Procedures for secure collection and maintenance of data
- Determination of who can have access to what data
- Providing data from the longitudinal student records system

This document builds on the contents of other documents, which are referenced at the conclusion, such as the *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies* and *Building an Automated Student Record System.* The Forum Guide contains a more complete overview of the federal laws relating to student records, as well as general guidelines for State and Local Education Agencies. The other document describes the steps that should be followed in order to develop a well-designed and useful system. This document on data access, however, goes beyond the other documents to offer more specific recommendations to State Education Agencies (SEAs) as they build their longitudinal student records systems.

Laws Requiring Protection of Student Records

Key Definitions

- ***Confidentiality* refers to an obligation not to disclose or transmit information to unauthorized parties.**
- ***Security* refers to technical procedures that ensure only authorized and intended parties have access to data.**
- ***Personally identifiable information* is data that can reveal an individual's identify.**
- ***Longitudinal student records system* is a computer system that contains individual student records linkable across school years and sites.**

The Family Educational Rights and Privacy Act (FERPA), passed by the U.S. Congress in 1974, provides for the protection of information about students and their families. It reinforces the right of education agencies to collect and maintain data about students, but it restricts the access to that information to educators with a "legitimate educational interest," i.e., the information is needed in order to carry out their professional responsibilities. In addition, FERPA gives the right of access to parents as well as the right to restrict release of the information in some instances. Federal education programs adhere to the requirements stated in FERPA, and great care is taken in the collection and release of student data by the United States government.

Other federal laws provide clarification and restrictions on the access to and use of student records, including the Individuals with Disabilities Education Act, the Richard B. Russell National School Lunch Act, the Children's Online Privacy Protection Act of 1998, and the Health Insurance Portability and Accountability Act of 1996. The reader is urged to review the discussion of these and other federal laws in the *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies.* The discussion in Section 2 of the *Forum Guide* is very complete and was written with assistance from USED.

Most states have passed laws that are similar to FERPA. Others have incorporated similar language into state rules and regulations. Most state laws and regulations address parent and student rights to have access to the student's records and restrict release of individual student information to certain situations.

Many state laws and regulations specify what types of data may be considered directory information, a distinction made in FERPA. Directory information generally is the information that appears in public documents such as school yearbooks, school rosters, athletic programs, and press releases concerning student honors. Directory information is considered the portion of the education record that would not generally be considered an invasion of privacy if disclosed, and it may include student and parents' names, address, and telephone number; school activities and

ESP Insight

Directory information is considered the portion of the education record that would not generally be considered an invasion of privacy if disclosed, and it may include student and parents' names, address, and telephone number; school activities and honors; height and weight of athletes; and degrees received.

honors; height and weight of athletes; and degrees received. Proposed regulations for FERPA include a student's user ID or other identifier used to access or communicate in electronic systems (e.g., email address) as directory information.

In some instances, state laws and regulations are more restrictive than FERPA. For instance, one state's law related to student records forbids release of the address and telephone information for elementary and secondary school students, such as in a school directory. Some states make mention of groups to whom student directory information may be released, such as military recruiters. States can have more restrictive laws and regulations, but they cannot be less restrictive than FERPA.

ESP Insight

States can have more restrictive laws and regulations, but they cannot be less restrictive than FERPA.

FERPA requires education agencies to have policies concerning education records and to notify parents and eligible students (students over the age of 18 or who are enrolled in postsecondary education programs) of their rights with regard to the student's education record. Most states leave the specifics of how this is done to the Local Education Agencies (LEAs), but some provide guidelines and sample policies and forms.

A question may arise as to whether a state's open records law is relevant to this discussion. Each state has its own open records law based on the Federal Freedom of Information Act (FOIA). As FOIA does for federal agencies, state open records laws direct state and local government agencies to make all records and data "available to the greatest extent possible, based on the principle of openness in government," unless restricted by some other statute. With regard to student records, FERPA is the relevant law, so restricted access to student records is crucial. But it behooves a State Education Agency to make as much information as possible available concerning the progress and success of public schools while maintaining the confidentiality of individual students' records.

The information in this document is meant to help a State (or Local) Education Agency to develop policies and procedures that will reassure students and their parents that access to the content of the student's record will be restricted according to best practices and federal and state laws and regulations.

Longitudinal Student Records Systems

Most State Education Agencies have begun to collect individual student records from Local Education Agencies. The data maintained in these longitudinal data systems includes information obtained from Local Education Agencies and information the state has access to directly, such as state assessment scores. LEAs are required to provide data for each student such as personal information, program participation information, courses taken, and other information. This is a subset of the information LEAs maintain about students in their student information systems (SIS) and other systems dealing with food programs, transportation, library usage, etc. Usually the data are collected on a periodic "snapshot" basis, but some State Education Agencies maintain "real-time" records of the students.

The purpose of the state longitudinal student records system is to provide essential information for monitoring progress of the schools and districts in meeting performance requirements for students. The information in the system is used for federal and state reporting related to programs and for funding the education system. Ideally, the State Education Agency (SEA) can use the system for doing research on what appear to be successful schools and the programs they offer. These systems also provide the capacity for handling *ad hoc* queries from state legislatures and others interested in the functioning of the education system. The longitudinal student records system should not be used, however, for locating individual children unless the SEA is directed to do this by the state's Attorney General.

ESP Insight
The purpose of the state longitudinal student records system is to provide essential information for monitoring progress of the schools and districts in meeting performance requirements for students.

One State's Written Purpose: **The student information system is intended to support better decision-making and policies for improving the performance of students and schools, reduce reporting burden (ultimately), help to facilitate the entry of students into a new district, and ensure that timely, high quality data are available to legitimate users.**

A key component of the longitudinal student records system is the capacity to track individual students across years and sites within the state. This requires a unique identifier and a means for schools to obtain the identifiers for students who move into the district. (Information on student identifiers can be found in the ESP Solutions Group *Optimal Reference Guide: Statewide Student Identifier Systems*.) Some states have used a student's Social Security Number (SSN) as the unique student identifier; however, we do not recommend that.

ESP Insight
A key component of the longitudinal student records system is the capacity to track individual students across years and sites within the state. This requires a unique identifier and a means for schools to obtain the identifiers for students who move into the district.

Issues regarding the ownership of the student records have been raised in working with a number of State Education Agencies. A **data owner** is the person who has the ultimate right to say what is true (e.g., the umpire owns the call on what is and is not a strike). The data owner may or may not maintain or control the actual data. Core demographic data about each student are "owned" by the student and/or his/her guardian (if white parents say their child is African American, then the student should be recorded as African American). Attendance, grade, and IEP data are "owned" by the school district where they originate. State assessment data are "owned" by the state. Such ownership distinctions do not impact access rights granted by FERPA.

Districts and states share stewardship responsibility for student data to fulfill state and federal reporting responsibilities. A **data steward** is the primary contact for an organization that is managing a particular set of data and is, therefore, responsible for ensuring standard data definitions are established and met and for securing appropriate access. As student record data stewards, they are responsible for providing all parties with "legitimate educational interests" with access to student records and data "to the greatest extent possible, based on the principle of openness in government."

Identifying Data for Inclusion in Longitudinal Student Records Systems

ESP Insight

A crucial beginning step in developing a state longitudinal student records system is deciding what data elements should be included about individual students.

A crucial beginning step in developing a state longitudinal student records system is deciding what data elements should be included about individual students. Categories of information maintained in local student records systems typically include: Personal information (e.g., demographic characteristics), membership (including enrollment, attendance, and completion), federal program participation, school program participation, school participation and activities, non-school and post-school experiences, assessment, transportation, food services, and health conditions. Discipline data are maintained in a variety of ways in the states. What is submitted to an SEA is a subset of the data in these categories. (More information about selecting data elements for inclusion may be found in the document *Building an Automated Student Record System.*)

It is important for an SEA to identify a data steward for different types of data. As noted above, the data steward should be knowledgeable about federal and state reporting requirements, and provide oversight for the accurate and complete collection of data. Efforts should be made to synchronize data between data stewards, particularly programs that use the same data elements, such as race/ethnicity, gender, and economically disadvantaged status. In general, an authoritative data source, such as the federal government, should trump other sources; however, inaccuracies should be corrected, wherever they reside.

ESP Insight

The SEA should develop a metadata dictionary containing all of the data elements included in the longitudinal student records system.

The SEA should develop a metadata dictionary containing all of the data elements included in the longitudinal student records system. Typically, this is a shared-application that contains a list of data elements with related metadata, such as definition, format, formulas used (if any), periodicity, uses, source, location, and access levels and conditions. Determining access levels will require careful consideration of the sensitivity of the data collected. (Access levels are covered below.) The metadata are essential for promoting data quality, as well as security.

Concerns about confidentiality of data in state longitudinal student records systems often relate to fear of having large amounts of sensitive personal data being kept in databases. SEA personnel identifying data elements for inclusion in a longitudinal student records system should select only those data elements that are crucial for reporting, analysis, and decision-making.

Procedures for Secure Collection of Data

The mechanisms used by the SEA to collect data from schools and districts must provide for the protection of the individual student data while in transit. Care must be taken at the local level to ensure that data entry and transfer are done by persons with a right to access and provide the data. This does not include students.

Electronic means of transmitting data are being used more and more, yet concerns about the safety of these means continue. While transfer of data using the Internet is generally considered safe, there are precautions that can be taken to promote confidentiality, such as encryption.

Longitudinal student records systems must contain data that have been provided by authenticated providers. This means that someone from each data provider, be it school or district, must have a secure means of logging into the system to upload the data. The data provider must be a trusted person identified by the school principal or district superintendent.

Persons responsible for enrolling students into a school or district must have a way to identify an existing unique student identifier or assign a new identifier so that the identifier can be attached to the student record that goes to the SEA. This means that trusted individuals must have secure access to a student identification locator system. This access is different than either the access needed to submit data and the access needed to view and use the data. The management of all types of access will be discussed more below.

ESP Insight
Persons responsible for enrolling students into a school or district must have a way to identify an existing student identifier or assign a new identifier so that the identifier can be attached to the student record that goes to the SEA.

Secure Maintenance of Student Data within the State Education Agency

There are many procedures that are needed to maintain a safe and secure longitudinal student records system. A crucial component is the decision about who can access the contents of the system, discussed below. However, other items that must be considered are the physical location of the hardware, software, and network containing the student records system, and how this location can be made secure from break-ins and potential disasters.

Databases must be kept secure from outside intruders through the use of passwords, firewalls, and other measures. Unauthorized changes to data must be avoided. Procedures should be in place to track who has access to student records and record when access is obtained. More detailed information on technology and security can be found in the *Forum Unified Education Technology Suite.*

ESP Insight
Databases must be kept secure from outside intruders through the use of passwords, firewalls, and other measures.

Determining Who Has Access to State Individual Student Records

Access to individual student records is allowed by FERPA for anyone with a "legitimate educational interest." This means that student records can be disclosed to school officials needing to review education records to fulfill their professional responsibilities without parental permission. For the most part, records are needed by educators that have daily contact with students, such as teachers, counselors, and administrators. Other officials within the school system may also have a need for individually identifiable information, but generally summary or aggregate data should serve their purposes. An SEA with a longitudinal student records system must develop a policy concerning access to student records, and define the criteria for determining what is a "legitimate educational interest" and what type of person has a "legitimate educational interest."

SEA Personnel. At least some SEA staff may be considered to have a "legitimate educational interest" in individual student records according to FERPA. However, decisions about individual children generally are not made at the state level, hence there is little need for SEA staff to have access to individually identifiable education records. On the other hand, SEA staff responsible for the education of students receiving special services (such as special education, vocational education, migrant education) may have a need to see individual students' records. Assessment specialists may have a need to look at individual student records to confirm scores or review other information such as eligibility for Title I. It is important to determine exactly who within the SEA, if anyone, must be able to obtain information on specific students from the central database.

For the longitudinal student records system to be used as an analytical tool, it is probably not necessary for anyone within the SEA to access an individual student's record, thus it makes sense to strip identifying information from the individual records and create an analysis file which will promote confidential maintenance of the data. It should be noted, however, that stripping name, address, and ID number from each student's record in the system does not guarantee that a student will be unrecognizable if the student has characteristics that are unique within his or her school or district. It will, however, provide a hurdle to potential intruders into the system. There is no sure way to remove all of the information that could identify an individual student other than encryption. Encryption, however, adds complexity to the legitimate use of the system. As a result, the best approach is to manage and secure access to the system. Users of the system must be informed of their responsibilities related to maintaining the confidentiality of the data.

ESP Insight

For the longitudinal student records system to be used as an analytical tool, it is probably not necessary for anyone within the SEA to access an individual student's record, thus it makes sense to strip identifying information from the individual records and create an analysis file which will promote confidential maintenance of the data.

Someone within the SEA (such as a system administrator) must have responsibility for ensuring the accuracy and completeness of the data submitted by the school districts. Checks should be made for data that fall outside of the expected range of information, for incorrectly formatted data, for combinations of data that seem suspicious (such as bogus students or unusual circumstances), and for incomplete sets of data. Verifications will be needed when records must be combined from different time periods. Someone will have to have access to the individual records within the system to be able to do these checks.

ESP Insight

Checks should be made for data that fall outside of the expected range of information, for incorrectly formatted data, for combinations of data that seem suspicious (such as bogus students or unusual circumstances), and for incomplete sets of data.

A database with individual student education records could be considered useful for a variety of purposes not intended by SEA staff. SEA staff may believe that the database is meant only to be used as a means of doing effective analytical studies and compiling data. Other people may see the database as the source of information about individual children. For instance, non-custodial parents may contact the SEA to find where their children are currently attending school. Legal opinions may be necessary to ensure that data are not released inappropriately. Staff will also need to know when and what data can be released.

LEA Personnel. Local Education Agency personnel have not traditionally been allowed access to state systems, as they should have copies of most if not all of the data within their own systems. However, the sophistication of the local data systems may not allow for the types of analysis that local educators might like to do with "their data." Also, there may be data in the state system that does not reside in the LEA system, and LEA educators might like to have access to these data. As a result, access for school and district personnel to their data in the state's longitudinal student records system is more important than ever. This access is allowed according to the proposed FERPA regulations.

A common assumption is that a principal (or his/her designee) should have access to information about all of the students in his/her school. Similarly, a district superintendent or designee should be able to see data about all of the students in his/her district. Besides providing access for submitting data to the state as mentioned above, access should be provided to review the data submitted to ensure that they are correct. In addition, access should be provided for use of analytical tools provided by the SEA to anyone approved by the district superintendent or school principal. This may include people such as school counselors, district research and evaluation personnel, and district finance officers.

Since the data compiled by the SEA may come from a variety of sources, the LEA may want to download a copy of all of their data for use at the local level. This will require very specialized technical access and approval from the district superintendent, but is not prohibited by FERPA.

Districts have "legitimate educational interests" about the students they serve, and, therefore, should be granted full access to all data in the SEA longitudinal student records system related to students currently enrolled in the district, including information before the enrollment period. It would be useful to have access to data about students previously enrolled in the district for the purpose of longitudinal analysis; however this is not addressed in the FERPA regulations, and may be prohibited.

Ideally, a school and district should be able to obtain information about a student's previous enrollments within the state and other relevant information from the state's longitudinal student records system. When a student moves today, usually only the information from the immediate past school/district is provided to the receiving school. Information about highly mobile student is useful to help schools better meet the student's needs.

Similarly, a school and district should be able to obtain information about what happens to a student after he/she is no longer enrolled in the school/district. For instance, when a student moves to another school just prior to when the state assessment is given, the sending school/district should be able to find out how that student performed. This is useful data for adjusting instructional programs. Also, it would be useful to know if a student graduated after moving from one high school/district to another. This information should be readily available to appropriate persons from the longitudinal student records system. However, it is not clear from the FERPA regulations whether such access would be allowable.

Researchers, consultants, and contractors. According to FERPA, personally identifiable information about students may be released without parental permission to persons or organizations outside of the SEA authorized to conduct research and evaluation studies or to contractors conducting data collection and maintenance activities for the State Education Agency. Authorization for researchers is for the purpose of increasing the existing body of knowledge about education in the state or conducting audits. Outside persons or organizations conducting research should be required to submit to the appropriate State Education Agency official a written request for permission to have access to personally identifiable data that explains the purpose of the research study and how the researchers will ensure data confidentiality and security. The release of student data to researchers outside the agency is considered a loan of data (i.e., the recipients do not have ownership of the data). Researchers should be required to destroy the data once the research is completed.

ESP Insight

According to FERPA, personally identifiable information about students may be released without parental permission to researchers authorized to conduct data processing or research and evaluation studies for the state education agency.

SEAs may contract with outside organizations to conduct data collection and maintenance activities which include personally identifiable student data. This is specifically noted as permissible in the new FERPA regulations. Outside organizations should be required to adhere to the SEA restrictions related to confidentiality and security of the data and should attest to that as a part of the contractual process.

Parents. Parents must be given access to the data maintained about their children within the state database. Upon the request of any student (or the student's parent/guardian if the individual is under the age of eighteen) under Section 99.20 of FERPA to gain access to his/her (child's) record contained in the student information system, the State Education Agency must provide a copy of all or any portion of the record in a comprehensible form. In addition, the SEA must consider requests to amend the record if requested by the parents or student. Since most of the data originate in the Local Education Agencies (and may be considered to belong to the Local Education Agencies), parents/guardians should seek first to review and amend the student's record through the Local Education Agency. The State Education Agency must have a policy for updating changes that come from the Local Education Agency or directly from the parents or student.

Others. Governors, lawmakers, state board of education members, and others may think that they have a right to gain access to individual student records. For instance, one state's legislature wanted to have access to a central student database so that its members could do studies to predict how many students would qualify for state-sponsored scholarships. Arrangements should be made to provide policy makers with the information they need rather than giving them access, thus protecting the confidentiality of student records.

Levels of Access

One way to document access is to determine levels of access from "Access to All Data" to "Access Only to Non-Identifiable Aggregate Data." Each staff position can be assigned a level based on whether he or she has a "legitimate educational interest." Full access must also be given to the technical managers and programmers responsible for making the system work. Staff should be trained on the SEA's acceptable use policy, and sign a document indicating they will abide by the rules of the policy.

Data elements should also be assigned levels of access from "Available to Anyone" to "Highly Restricted." Data elements considered "directory elements" are generally available to anyone. Test scores, health information, and other types of evaluation data should be considered highly confidential. Assignment of levels of data access to levels of staff access can be by data category or for each data element.

ESP Insight
Data elements should also be assigned levels of access from "Available to Anyone" to "Highly Restricted."

The following table shows how staff members can be assigned access to data categories.

Student Data Sections	SEA Chief	Current LEA Admin to Current Data	Current LEA Admin to Past Data	Past LEA Admin to Later Data	Current Teacher to Current Data	Current Teacher to Past Data	Past Teacher to Later Data
Personal Information	🟦	🟦	🟦	🟨	🟨	🟨	🟨
Membership	🟦	🟦	🟦	🟨	🟦	🟨	🟨
Federal Program Participation (EDEN)	🟦	🟦	🟦	🟨	🟦	🟨	🟨
School Program Participation	🟦	🟦	🟦	🟨	🟦	🟨	🟨
School Participation and Activities	🟦	🟦	🟦	🟨	🟦	🟨	🟨
Non-School and Post-School Experiences	🟦	🟦	🟦	🟨	🟦	🟨	🟨
Assessment	🟦	🟦	🟦	🟦	🟦	🟦	🟦
Transportation	🟦	🟦	🟦	🟨	🟦	🟨	🟨
Food Services	🟦	🟦	🟦	🟩	🟦	🟩	🟩
Health Conditions	🟦	🟦	🟨	🟩	🟩	🟩	🟩
Civil Rights Survey Data	🟦	🟦	🟨	🟩	🟩	🟩	🟩

🟦 Access to data in a category for all students in the district or school for whom responsible.

🟨 Access to all data in a category, but only for their students (present or past).

🟩 No access to the data for any students.

Following is a listing of data levels developed by one State Education Agency.

Levels of Access to Data in the Student Information System

It is useful to think of a single record of an individual student as a folder that contains many pieces of information, such as name, school building number, gender, or date of birth, etc. These are called fields. Every field in the student information system is assigned an access level between 1 and 4, with Level 1 being the highest level. All access levels are assigned in a way that maximizes usage by educators without risking inappropriate disclosure of personally identifiable information.

Level 1 Access allows authorized SEA staff to read and write to all the records and fields in the database. This level is only permitted to a minimal number of authorized staff members who operate or manage the database or are responsible for maintaining the accuracy, security, and audit corrections in the performance of their duties. Authorization by the student record system manager will be required for this level of access.

Level 2 Access places limits on access to individual records but not fields. Specifically, superintendents (or their designees) of local school districts will have read-and-resubmit access to records of their own students. Another way to say this is that a superintendent may see all of the fields (data) collected about any of the students in his or her school district and can direct that data be resubmitted if errors are identified.

Level 3 Access provides school principals (or their designees) with access to data about their students for the current and previous years. This is a proposed function of the system that would allow comparisons of student scores and other data across school years and school districts for use in decision making about instructional improvements. In addition, this level of access would allow principals to obtain information about the performance of their former students who have gone on to postsecondary education, should this arrangement be available.

Level 4 Access gives read-only access to a limited set of fields for all students within the State. The purpose of this level is to allow designated district personnel who are responsible for registering new students to determine a student's ID through use of a student locator system. Information that could help to better place a new student for instruction may be included. This is consistent with FERPA Section 99.31(a)(2).

Some SEA staff responsible for audits, operations, accreditation, and reporting to State and federal government agencies will have access to a limited set of fields, excluding student names. The fields that are available at level 3 will be specified in an appendix once they are identified.

Public read-only access may be made available to the general public, including educational associations, media, real estate agents, businesses, interest groups, etc., to view standard reports and data tables that are produced and published in aggregated formats on the Web. Data on individual students **will not** be accessed by anyone at this read-only level.

It is possible that some of the reports available through public read-only access would be based on a very small population of students or educational personnel, which could reveal information about the individuals in that group. For instance, if a search were done for the math scores of all Asian/Pacific Islanders, and this search revealed two students in a particular building, there would be some certainty that information about an individual could be disclosed. Therefore, the student information system manager will block any aggregate results with a statistical cutoff in which fewer than **ten** students might be disclosed.

Providing Data from the Longitudinal Student Records System

States have moved toward developing longitudinal student records systems because of the need to hold schools and districts accountable for student performance. The *No Child Left Behind Act's* regulations require states to monitor performance of subgroups of students such as those who are economically disadvantaged, limited English proficient, migrant, or homeless. Many of the students fall into more than one of these categories, thus accounting becomes more difficult and duplicative if data are aggregated separately for submission to the state. By having individual student records, a state can "slice and dice" the data anyway that is needed. There may be other subgroups of interest in a state than those required by federal law. Thus, the state's longitudinal student records system provides for aggregating the data needed for federal and state reporting, as well as giving the state an analytical database for identifying problems and successes.

ESP Insight

The state's longitudinal student records system provides for aggregating the data needed for federal and state reporting, as well as giving the state an analytical database for identifying problems and successes.

Aggregate statistics compiled from the student record system do not necessarily mask the identity of children if the children have unusual characteristics within their schools or districts. If assessment scores are presented by race/ethnicity within a school and there is only one Asian/Pacific Islander in the school, then it is obvious that student received the score reported in that portion (cell) of the table. If there are scores for two students within a cell, then knowing one score would enable a person to figure out the other student's score. Including a minimum of three students in a group (cell) should prevent this type of inappropriate release of information from occurring. Higher minimums increase the number of students that must be known before the value for the final student can be calculated, thus are safer. For more information on selecting appropriate group sizes, see the ESP Solutions Group *Optimal Reference guide: Confidentiality and Reliability Rules for Reporting Education Data*.

General Recommendations for Protecting the Confidentiality of Education Records Maintained at the State Education Agency

1. Develop a policy statement that describes the purpose of the Student Information Management System, the appropriate usage of individual student data within the State Education Agency, and conditions for release of data contained within the database. Include information about statutory requirements and expectations for the system.

   In general, states that have individual records do not have them to track individual students and make specific decisions about them, although that could be done. Decisions about individual students are usually made at the local level where the students attend school. Decisions made with a state database are focused on groups of students, such as students who are economically disadvantaged, disabled, non-English speakers, migrants, and gifted. Data are used to monitor instructional quality, equity, and achievement. Monitoring progress of students within schools and districts over time is an important use of such databases; so being able to link records from year to year is essential. A unique student identifier is needed to ensure records can be accurately linked from year to year.

   The policy statement containing the goal and planned uses of the state database must be provided to the staff of the SEA, and those with access to the database must be aware of restrictions to its use and penalties for misuse. In addition the policy statement should be made available to lawmakers and citizens of the state.

ESP Insight
Monitoring progress of students within schools and districts over time is an important use of such databases; so being able to link records from year to year is essential.

2. Identify all persons within the State Education Agency who must or will have access to the Student Information Management System. Determine the data elements to which they must or may have access. These persons include:

   - Persons who must have access to the database for monitoring the progress of individual students or for special studies about groups of students.
   - Persons who will have responsibility for monitoring the quality of the student data submitted by Local Education Agencies. These persons may have responsibility for removing individually identifiable information and replacing identifiers with substitutes, merging new data sets with previous data sets, checking for data quality (e.g., data that appear outside of the range of expected data or nonsense data), and consulting with LEAs about the content or quality of their data. These may be technical or program level staff.
   - Persons who must consult with LEAs about the electronic transmission of data. These will be technical persons with the responsibility for helping the LEA staff to transmit the data using secure procedures.

3. Develop a policy statement that specifies the restrictions under which these groups of SEA staff are allowed access to the database and any penalties they

may suffer for inappropriate use of the database or release of the data. Make sure that all staff in these positions are trained and knowledgeable about their responsibilities related to confidentiality, their abilities to access and use the data, and the procedures to use if they are asked to perform duties beyond the stated requirements. While not required in federal and state law, staff members can be asked to sign a statement indicating that they:

- acknowledge the purpose, restrictions, and appropriate uses of the database,
- understand the penalties for misuse and unauthorized disclosure of the data, and
- agree to the ethical and legal requirements to maintain the confidentiality of the data.

4. Develop a policy statement that specifies what data will be collected and why these data are to be collected. Make sure that any data elements you collect about individual students can be justified from legal and ethical standpoints. In order to identify what data are needed, review the data needs for the State Education Agency, including federal and state reporting, funds distribution, accreditation, accountability, and any other relevant requirements. Determine which data are best obtained through analysis of individual student education records. Make sure that LEAs understand why the data are needed and how they will be used.

5. Develop policies and procedures that will help to ensure proper collection of the data at the local and state levels, and that will ensure confidentiality of the data. The policies should be an extension of existing policies at the local level where the data are originally collected. Local Education Agencies are responsible for providing complete data for their students.

   Collecting student level data into a centralized database will require a combination of methodologies. School districts with automated student record systems will probably want to download the desired data from their computer files. These districts should have trusted computer programmers who can handle the movement of data from the central database to the State Education Agency in a confidential manner. SEA staff should work with the district's staff to ensure that proper format crosswalking is accomplished, that data are submitted in the proper order, and that the procedures used require as little re-keying of data as possible. Well-done computer crosswalks may result in fewer errors and problems.

   Since many districts still keep data in paper files, the data elements requested by the State Education Agency will have to be manually entered into a computer file. Guidelines and procedures should be developed that will help these districts determine the best ways to get the data entered into a computer file while maintaining confidentiality. For instance, guidelines should specify who would be appropriate to do data entry. Many schools use students as office assistants. Students should not be used, however, to key in data of other students. Similarly, parent volunteers are not appropriate.

ESP Insight
Well-done computer crosswalks may result in fewer errors and problems.

If a district is obtaining a computer specifically for providing the data to the State Education Agency, suggestions might be made as to what type of equipment would be needed, where it should be maintained, security measures that might be needed, who should be allow to use it, etc. For small districts not currently using computers for administrative student record keeping, these suggestions should be welcome.

Some State Education Agencies have found it useful to develop custom computer software that can be used for entering data into the desired format. In addition, procedures are needed to collect the data via the internet or direct connections. Carefully designed procedures help to ensure that data are comparable and complete, but are also essential to ensure that confidentiality is maintained. If contractors are used to design state databases with student data, these procedures need to be developed collaboratively, with significant input from SEA staff.

ESP Insight
Carefully designed procedures help to ensure that data are comparable and complete, but are also essential to ensure that confidentiality is maintained.

6. Develop procedures that will ensure secure maintenance of student data within the State Education Agency. Computer access restrictions and procedures are needed to promote data confidentiality. Prohibiting access through the use of passwords, firewalls, and other technical means will help to ensure that only those with a "need to know" can see individually identifiable data. Remind staff members of their responsibility to ensure no one else has access to the database when they leave their desks.

   It is crucial to review internal physical access to the computer and develop appropriate security measures. The computer containing the database should be located where unauthorized persons will not have access, and where physical problems or disasters (e.g., broken water pipes, electrical shortages) are not likely to compromise the security of the computer. In addition, measures are needed to prevent theft. Security of the equipment is essential. This is also crucial for data maintained offsite in a contractor's location.

   A major threat to confidentiality is unauthorized access from outside the agency; therefore, another type of security must be considered. When computers can be accessed through direct dial-up modem or Internet access, there is the potential for outside intruders to access and manipulate the data. Outside access must be denied through the use of firewalls, password access, and careful monitoring of computer activity. Removal of basic student identifying information from the database will present a hurdle to unwanted intruders trying to locate specific students' records.

ESP Insight
A major threat to confidentiality is unauthorized access from outside the agency; therefore, another type of security must be considered.

7. Develop rules and procedures concerning the proper usage and release of student data. Document the policies and procedures for maintaining confidentiality and appropriate usage within the State Education Agency, and be prepared to make it available to parents, the press, state lawmakers, and others within the public whenever necessary. Not all of the specific procedures need be spelled out for the reader, but a general discussion of policies and procedures can be reassuring to parents and others.

SEAs must develop procedures for allowing parents to have access to the data maintained about their child within the database. Some states have the means to print out a listing of the information about any one child when a parent asks to see what is there. Other states have districts provide this information to the parents, since the data maintained in the state database is identical to the data maintained at the local level. Even state assessment data can be provided through Local Education Agencies. Providing information through the district is less intrusive and burdensome for the SEA and may be easier for the parent who does not have to travel to the state capital.

Identify a person or office to which all requests for release of information must go. There may be requests from the courts, parents, and certain governmental agencies for individual student data.   Some people will call several people within a State Education Agency trying to get the answer they want, rather than just taking the word of the first person who answers the questions. Because of the confidential nature of the contents of this database, it is important to have a single office responsible for ensuring appropriate maintenance and usage of the database. Unusual requests may require additional assistance from legal staff or the state's Attorney General.

ESP Insight
SEAs should plan ahead for the types of data requests they may receive.

SEAs should plan ahead for the types of data requests they may receive. For instance, state lawmakers and board members may want to obtain access to the database in order to do analyses. One solution is to have SEA staff dedicated to doing these types of analyses in response to requests. A more effective way is to anticipate the types of studies that may be requested and provide report generating capability to persons outside of the agency (and for insiders, too). Still another way to handle requests for access to this rich database is to create a research/public data extract from the statewide database including only those data elements determined to meet criteria set by the SEA relating to confidentiality. Such a data extract would, of necessity, have to have important personally identifiable information removed, such as race/ethnicity, school, or other information that could identify an individual student. Hence the utility of the data extract might be less than desired.

ESP Insight
We recommend a minimum of between three and five students per cell for public reporting of sensitive data, such as achievement scores.

It is most likely that data released from the database will be in an aggregate format at the school or district level. Data might be compiled for groups of students, such as Title I students, transitional bilingual education students, and other groups receiving special services. Assessment scores are generally released as averages, ranges, or numbers of students meeting specific proficiency levels. In general, these data will not be personally identifiable; however they could be. As a result, the SEA must develop a policy relating to the release of statistical data in a confidential manner. Many education agencies set a specific minimum cell size, or number of students for whom averages are reported. As mentioned earlier in this paper, the SEA might choose to require a minimum of three students in a cell for public reporting purposes. If the minimum number is set too high, then useful information may not get reported. Setting a higher minimum number, on the other hand, provides more security that the individual students' data might be discovered. This is an issue with no clear-cut answer. We recommend a minimum of between three and five students per cell for public reporting of sensitive data, such as achievement scores. For use in monitoring quality at individual schools, actual data can be used as long as it is not released to the public.

Specific Recommendations

1. Develop a policy statement that describes the purpose of the Student Information Management System, the appropriate usage of individual student data within the SEA, and conditions for release of data contained within the database. Train all SEA staff on the contents of this statement. Release the statement to lawmakers and citizens of the state.

   Make a list of all persons or positions within the SEA who must or will have access to the Student Information Management System and the data elements they may access. Document their roles and responsibilities with regard to the system and maintaining the confidentiality of the contents.

2. Develop a document that can be provided to school, LEAs, and parents containing the listing of what data elements will be collected and when they will be collected if they are to be implemented in phases. Also describe the reasons why the data elements are to be collected and standard reports to be produced. Provide information about how access to the data elements will be restricted.

3. Develop and document procedures to limit access to the central student database to only those persons identified as having a need to know. Assign special passwords to those who can access the data. Develop a system that will log when and by whom the database is accessed and changes to the database are made.

4. With the help of LEAs, develop procedures for allowing parents to have access to the data maintained about their children in the state database. Design a form that parents complete to request access to their child's record. Verify by photo identification that the parents are who they say they are or have the district do this. Arrange for parents to receive a copy of the contents of their child's state record from the Local Education Agency where the student attends. Make sure that LEAs have a copy of all information kept in the state database about their students, including state assessment data. Designate a person or office in the SEA to receive the requests and arrange for the information to be shared with the parents in the LEA.

5. Develop a set of "canned" reports that can be run on the database to produce the types of studies that most frequently will be requested. Determine who within the SEA can run reports, and whether or nor anyone from outside of the agency will be allowed to run the reports.

6. Establish standards for the release of data from the database. Specifically, make sure that there are no fewer than three students in a group for which data will be reported. Review statistical reports carefully to determine if the data being released in different reports could together be used to identify data about individual students.

7. Develop procedures for sharing student data with researchers, contractors or other organizations, such as a state higher education agency. Develop

documentation that ensures that persons gaining access to student records are knowledgeable about restrictions on inappropriate disclosure of student data and the means needed to ensure confidentiality and security.

Summary

Restricting access to individual students' records is important whether the data are maintained at the classroom, school, district, state, or federal level. The development of a set of detailed and carefully crafted policies and procedures at the State Education Agency level will help to avoid improper disclosures where the data are maintained and alleviate the concerns of parents, students and the public as a whole. These policies and procedures should refer to who has access to the data, what data will be maintained, what are the uses of the data, and what will be done to ensure secure data collection and maintenance.

References

Ligon, G. 1996. "New Development in Technology: Implications for Collecting, Storing, Retrieving, and Disseminating National Data for Education." *U.S. Department of Education, National Center for Education Statistics, From Data to Information, New Directions for the National Center for Education Statistics:* 9.32-65

ESP Solutions Group. 2005. *The Optimal Resource Guide: Confidentiality and Reliability Rules for Reporting Education Data.*

ESP Solutions Group. 2005. *The Optimal Resource Guide: Statewide Student Identifier Systems.*

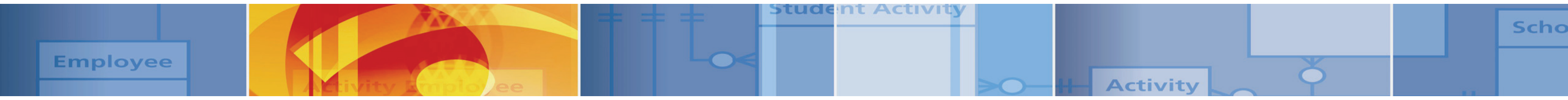
ESP Solutions Group. 2006. *What's Really "In Store" for your Data Warehouse, Part I.*

ESP Solutions Group. 2006. *What's Behind Your Data Warehouse? Part II.*

National Forum on Education Statistics. 2004. *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies,* NCES 2004-330. Washington, DC.

National Forum on Education Statistics. *Forum Unified Technology Suite*. http://nces.ed.gov/pubs2005/tech_suite/

U.S. Department of Education, National Center for Education Statistics, National Forum on Education Statistics. 2000. *Building an Automated Student Record System.* NCES 2000-324. Project Officer: Beth Young. Washington, DC.



About ESP Solutions Group

ESP Solutions Group provides its clients with *Extraordinary Insight*™ into K-12 education data systems and psychometrics. Our team is comprised of industry experts who pioneered the concept of "data driven decision making" and now help optimize the management of our clients' state and local education agencies.

ESP personnel have advised school districts, all 52 state education agencies, and the U.S. Department of Education on the practice of K-12 school data management. We are regarded as leading experts in understanding the data and technology implications of the **No Child Left Behind Act (NCLB)**, **Education Data Exchange Network (EDEN)**, and the Schools **Interoperability Framework (SIF).**

Dozens of education agencies have hired ESP to design and build their student record collection systems, federal reporting systems, student identifier systems, data dictionaries, evaluation/assessment programs and data management/analysis systems.

To learn how ESP can give your agency *Extraordinary Insight*™ into your K-12 education data, contact ESP at (512) 879-5300 or info@espsg.com.

This document is part of *The Optimal Reference Guide* Series, designed to help education data decision makers analyze, manage, and share data in the 21st Century.

ESP Solutions Group

(512) 879-5329
www.espsolutionsgroup.com
Austin • Boston • Washington DC