ies NATIONAL CENTER FOR EDUCATION STATISTICS
Institute of Education Sciences

SLDS Technical Brief

Guidance for Statewide Longitudinal Data Systems (SLDS)

November 2010, Brief 2
NCES 2011-602

Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records

Contents

SLDS Technical Briefs are intended to provide "best practices" for consideration by states developing Statewide Longitudinal Data Systems.

For more information, contact:
Marilyn Seastrom
National Center for Education Statistics
(202) 502-7303
Marilyn.Seastrom@ed.gov

The growth of electronic student data in America's education system has focused attention on the ways these data are collected, processed, stored, and used. The use of records in Statewide Longitudinal Data Systems to follow the progress of individual students over time requires maintaining student education records that include information that identifies individual students. The sensitivity of some of the personally identifiable information in student records increases the level of concern over these data. Administrators and data managers can help ensure the protection of personally identifiable information in the student records they maintain by developing and implementing a privacy and data protection program. The principles embodied in the Fair Information Practices adopted in the United States by the Federal Chief Information Officers Council and the Department of Homeland Security, coupled with the Family Educational Rights and Privacy Act (FERPA) and related regulations, provide a foundation for such a program.

Data Stewardship Defined

In 1973, the Department of Health Education and Welfare (HEW) report *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* discussed the need to "maintain data in the system with such accuracy, completeness, timeliness, and pertinence as is necessary to assure accuracy and fairness in any determination relating to an individual's qualifications, character, rights, opportunities, or benefits that may be made on the basis of such data" (pg. 6, Chapter IV). This was codified in the Privacy Act of 1974 (5 U.S.C. § 552a(g)(1)(C). More recently, on their website, the American Statistical Association's Committee on Privacy and Confidentiality cites the Census Bureau's definition of data stewardship as an "organizational commitment to ensure that identifiable information is collected, maintained, used, and disseminated in a way that respects privacy, ensures confidentiality and security, reduces reporting burden, and promotes access to statistical data for public policy." These two sets of requirements can be combined and tailored to education data as follows:

> Data stewardship is an organizational commitment to ensure that data in education records, including personally identifiable information:
>
> » Are accurate, complete, timely, and relevant for the intended purpose;
>
> » Are collected, maintained, used, and disseminated in a way that respects privacy and ensures confidentiality and security;
>
> » Meet the goals of promoting access to the data for evaluating and monitoring educational progress and educational programs; and
>
> » Meet the goals of assuring accuracy to ensure that decisions relating to an individual student's rights and educational opportunities are based on the best possible information.

These requirements are best operationalized through written policies and procedures. Typically, in a system with multiple uses and users, the task of establishing and promulgating policies and procedures is assigned to a Governance Committee that includes representatives of management, legal counsel, the data system administrator, data providers, data managers, and data users. The members representing these different stakeholders should be appointed to the Governance Committee by the head of the state education office, school district, or school, depending on the level where the affected data are held. This group should be established to work collaboratively to develop the policies and procedures for a privacy and data protection program. These policies would then be implemented by the data system administrator through the ongoing management of data collection, processing, storage, maintenance, and use of student records. Any appeals of the established policies and procedures should be directed to the appointing official.

In developing a statewide longitudinal data system, privacy and data protection plans must be in place in each entity that holds student records with personally identifiable information. This includes, for example, preschools, elementary and secondary schools, postsecondary programs and institutions, and workforce training programs. It also includes different organizational levels within each of these components of the education system; for example, elementary and secondary school data are typically held at the school, district, and state levels. Whether they are developed separately at each level or as a part of a unified approach across levels, efforts must be undertaken to ensure that the policies and rules and regulations are compatible across levels. For example, in elementary and secondary education, there may be more information maintained in a student education record at the school and district level than is planned at the state level. In this case, if the privacy and data protection plans are being developed and promulgated from the state level, districts and schools must supplement their plans to ensure that all personally identifiable information maintained about their students is included. On the other hand, if each education level is developing privacy and data protection plans separately, efforts must be undertaken to ensure that established policies and procedures are complementary and do not conflict.

Conduct an Inventory of Personally Identifiable Information

In order to ensure that the necessary data protections are in place, the Governance Committee or a Data Subcommittee for each entity that holds student records must first identify the personally identifiable data elements that need to be protected. Personally identifiable information (PII) includes information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. In the case of education data, FERPA regulations (34 CFR § 99.3).

The term personally identifiable information includes, but is not limited to:

1. The student's name;
2. The name of the student's parent or other family members;
3. The address of the student or student's family;
4. A personal identifier, such as the student's Social Security Number, student number, or biometric record;
5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and/or
7. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. (34 CFR § 99.3)

In conducting the inventory, the specific use of PII must be taken into account. For example, while FERPA has provisions to protect students' right to privacy, including the right to inspect and review education records (20 U.S.C. § 1232 (a); 34 CFR § 99.10) and a requirement for consent to disclose information to unauthorized entities (20 U.S.C. § 1232 (b); 34 CFR § 99.30), FERPA permits the release of student directory information[1] (20 U.S.C. § 1232g(a)(5); 34 CFR § 99.3). A school directory may include PII such as a student's name, grade level, and contact information. Taken by itself, the release of this information is not harmful to a student. However, when combined with the student's Social Security Number or another identifier and the student's education record, this information has the potential for violating a student's right to privacy. The release of this combined record could lead to harm or embarrassment. Thus, the privacy and data protection program should focus on PII that will be maintained in the electronic student record system with its likely wealth of student data.[2]

Identify All Personally Identifiable and Sensitive Information

The inventory should include all current and proposed data elements (National Institute of Standards and Technology [NIST], *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, pg. 2-2). It should also identify both direct and indirect identifiers. *Direct identifiers* provide information that is unique to the student or the student's family (e.g., name, address, Social Security Number, other unique education-based identification number, photograph, fingerprints, or other biometric record). *Indirect identifiers* are not unique to the student or the student's family but can be used in combination with other information about the student to identify a specific student (e.g., racial or ethnic identity, date of birth, place of birth, mother's maiden name, grade level, participation in a specific program, course enrollment).

An analysis of indirect identifiers should consider the likelihood of identifying an individual student both as a result of a combination of multiple data elements included in the student's education record and as a result of linking the information in education records to information included in external databases. In the first instance, a combination of data elements within student education records might reveal that there is only one student in a specific grade within a school with a set of observable characteristics who experienced a negative academic outcome (e.g., one Hispanic third-grader receiving instruction as an English language learner failed to reach the *proficient* performance level on the state reading assessment). In the second instance, if an external database contains enough overlapping data elements that are unique to an individual student, the two databases can be linked and any additional PII included in the external database can then be associated with that student's education record.

Linkage with information from an external source could occur as a result of a direct linkage by someone with access to two confidential data systems who is able to directly link the two databases (e.g., the student record linked to local public health records on sexually transmitted diseases or local crime records) or as a result of a less direct linkage of information from a student's education record with information available in public records (e.g., the education record for a 15-year-old Asian female includes participation in services for unmarried pregnant students, and public birth records could be used to identify the father of the student's child. Alternatively, an education record might show that a 13-year-old female student was the victim of a violent assault during the school day on a specific date (without the specifics of the assault). Meanwhile, a report in a local newspaper, while protecting the direct identifiers of the victim, reveals some of the details of an assault on a female student in that school on the same date).

At the elementary and secondary level, an analysis of the indirect identifiers should also consider whether any of the data elements are protected under the Protection of Pupil Rights Amendment (PPRA) (20 U.S.C. § 1232h; 34 CFR § Part 98). To protect the privacy and related rights of

[1] Educational agencies or institutions are granted the authority, under FERPA, to publicly release directory information after providing public notice to the parents of students or to eligible students in attendance at the agency or institution of the types of personally identifiable information that the agency or institution has designated as directory information. The parent or the eligible student must also be given the right to refuse to have any or all of the student's information released as directory information.

[2] An electronic student record system, or information system, consists of a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of [education] information. (44 U.S.C. § 3502)

students and parents, the PPRA requires written parental consent before a minor student can be required to participate in any survey, analysis, or evaluation funded by the U.S. Department of Education that includes information concerning the following:[3]

1. Political affiliations or beliefs of the student or parent;
2. Mental and psychological problems of the student or the student's family;
3. Sex behavior or attitudes;
4. Illegal, anti-social, self-incriminating, and demeaning behavior;
5. Critical appraisals of other individuals with whom respondents have close family relationships;
6. Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
7. Religious practices, affiliations, or beliefs of the student or the student's parent; or
8. Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

In the event any data elements under consideration for inclusion in a student record system involve any of these eight topics, those data elements should be included on the inventory of PII and should be identified on the list as PPRA-related variables.

A number of data systems include data on students' instructors. A teacher identification number, a student-teacher link, and information on the teacher's education, certification, teaching assignments, and scores on teacher assessments are examples of the types of teacher data elements that may be included at the preschool, elementary, and secondary levels. A faculty identification number, a student-faculty link, and information on the faculty member's field, education, tenure status, credit hours taught in the relevant academic period, and amount of funded research may be included at the postsecondary level. Although FERPA and the definitions given refer specifically to students, PII on teachers and any other staff that are maintained as part of the electronic record system should be included in the inventory of PII and protected in the same way as the student data. Apart from the fact that protecting any PII is a best practice, when faculty and staff data are linked to the student's record, they become indirect identifiers for the student record and can be used to identify individual students.

[3] Under PPRA (20 U.S.C. § 1232h; 34 CFR Part 98), school districts receiving funds from the U.S. Department of Education are required to provide annual parental notification of their policies concerning students' rights and of the specific or approximate dates during the school year of any survey that is scheduled to be administered to students if the survey includes any of the eight restricted topics, regardless of survey funding.

Confirm the Need to Maintain Personally Identifiable Information

The Fair Information Practice of *Data Minimization and Retention* calls for "only collecting personally identifiable information that is directly relevant and necessary to accomplish the specified purpose(s). [And for] only retaining personally identifiable information for as long as is necessary to fulfill the specified purpose(s)." In addition, the Fair Information Practice of *Purpose Specification* calls for "…specifically articulating the purpose or purposes for which the PII is intended to be used." Once the list of current or planned PII in an education record is completed, the planned uses should be identified for each data element (NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, pg. 3–4). Decisions should be made as to whether each data element is needed.

The National Forum on Education Statistics[4] identified the following K–12 administrative uses of student education records in the 2004 report *Forum Guide to Protecting the Privacy of Student Information: State and Local Agencies* (pg. 44):

» INSTRUCTION—Teacher and counselors need information about an individual student's previous educational experiences and any special needs the student might have to deliver appropriate instruction and services and to plan educational programs; parent contact information is needed to keep parents informed of student progress.

» OPERATIONS—Schools and districts need data for individual students to ensure the efficiency of day-to-day functions such as attendance records, meeting individual students' special needs, handling individual students' health problems, and operating food service and transportation programs.

» MANAGEMENT—Schools, districts, and state education agencies use data about students for planning and scheduling educational programs and for the distribution of resources.

» ACCOUNTABILITY—Schools, districts, and state education agencies use data about students and about individual students' progress to provide information about students' accomplishments and the effectiveness of schools and specific educational programs.

» RESEARCH AND EVALUATION—Schools, local, state, and federal education agencies use data about students and about individual students' progress to conduct analysis of program effectiveness, the success of student subgroups, and changes in achievement over time to identify effective instructional strategies and to promote school improvement.

Recent legislative initiatives provide funds for states to develop and implement statewide longitudinal data systems to support data-driven decisions to improve student learning and to facilitate research to increase student achievement and close achievement gaps.[5] These data systems are intended to enhance the ability of states to manage, analyze, and use education data. The supporting legislation calls for an expansion in the amount of information included in student education records, including linkable student and teacher identification numbers and student and teacher information on student-level enrollment, demographics, program participation, test records, transcript information, college readiness test scores, successful transition to postsecondary programs, enrollment in postsecondary remedial courses, and entries and exits from various levels of the education system. To facilitate the usefulness of this information, the legislation also calls for an alignment between P–12 and postsecondary data systems, which requires linkages between student and teacher records, between preschool and elementary education, and between secondary and postsecondary education and the workforce.[6] These linkages require data sharing across different components of the education system.

[4] This entity is a part of the National Cooperative Education Statistics System, which is authorized in law (20 U.S.C. § 9547). It was established and is supported by the National Center for Education Statistics for the purpose of assisting in producing and maintaining comparable and uniform information and data on early childhood education and elementary and secondary education. To this end, the National Forum proposes principles of good practice to assist state and local education agencies.

[5] Educational Technical Assistance Act of 2002, Title II of ESRA, 20 U.S C. § 9607.

[6] The America COMPETES Act, 20 U.S.C. § 9871 identifies data elements that are important in statewide longitudinal data systems, Title VIII of the American Recovery and Reinvestment Act of 2009 (ARRA, Pub. L. 111-5), authorizes funds to the Institute of Education Sciences to carry out section 208 of the Educational Technical Assistance Act, $250,000,000, which may be used for Statewide data systems that include postsecondary and workforce information, and Title XIV of this Act requires states accepting funds under this Act to establish statewide longitudinal data systems that incorporate the data elements described in the America Competes Act.

Some of the uses of education data require PII from individual students' records; others use aggregated student data for one point in time that are derived from information included in education records; others use aggregate student data that are derived from longitudinal data on individual students; still others use individual student level data linked across levels of the education system. Thus, some uses require access to PII, including the students' names and contact information, and, in some cases, linked longitudinal data; some may require detailed linked longitudinal data included in student records but do not require access to the individual students' names or other direct identifiers; still others may require nothing more than aggregates of data for a single year, again with no need for any information on individual students. Lists of the specific anticipated uses and linkages of the data can help to clarify data needs and to identify those needs which do or do not require access to PII. In addition, given the utility of linking data across sectors, care should be taken to ensure that the direct identifiers that are needed for accurate linking across record systems are maintained.

The length of time student records are retained is complicated by the fact that students may need to request information from education records as proof of credentials for employment purposes over the course of their workforce careers. To protect student privacy, while at the same time maintaining student records, the Governance Committee should develop a schedule and plan for migrating student education records to a retrievable archive following a student's completion at a specific level or departure due to transferring or dropping out. This would preserve the student education records for use in documenting a student's educational credentials (e.g., grade level and/or courses completed and grades or scores earned, honors conferred) and would allow for linkages across sectors and for retrospective evaluations of educational progress. At the same time, archiving historic student education records in a secure environment that is separate from the currently active components of an electronic student record system decreases the likelihood of unauthorized or inadvertent disclosures of records belonging to former students. Similarly, the Governance Committee should establish a plan for record destruction at such point in time when it is anticipated that the records will no longer be needed.

Ensure Data Quality and Integrity

The Fair Information Practice of *Data Quality and Integrity* calls for "ensuring, to the greatest extent possible, that personally identifiable information is accurate, relevant, timely, and complete for the purposes for which it is to be used." The issue of relevance will have already been addressed in the review of the specific uses and need for individual data items. Once a decision is reached to maintain a specific data element in students' education records, there is an obligation to ensure that the information included is up to date and complete and that it accurately reflects the students' educational experiences. Systems should be put in place to ensure the regular periodic updating of student education records with the most current and accurate information available for the intended purpose (e.g., an annual review and updating of student course transcripts). In fact, in recognition of the importance of these elements of student privacy, FERPA (20 U.S.C. § 1232g (a) and the related regulations (34 CFR § 99) acknowledge the right of a parent to inspect and review his or her child's (or, in the case of an eligible student, his or her own) education record for accuracy and to ensure that there are no violations of privacy with the right to request a correction or amendment.

Identify the Risk Level Associated with Different Types of Personally Identifiable Information

Not all personally identifiable data have the same level of sensitivity.[7] Some personally identifiable data elements are more identifiable and/or more sensitive than others and may thus require more electronic security and more controls on access to the data elements. To guide the organization's use of PII and the protections provided for such data, the Governing Committee or the Data Subcommittee should also evaluate the risk of harm associated with each personally identifiable data element. All PII included in a student education record system must be protected, but some may require additional protections (e.g., Social Security Numbers, disciplinary record, medical records).

[7] Sensitivity should be evaluated both in terms of the specific data element and other available personally identifiable data elements. Note that an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or ZIP code.

PII that is unique to a specific individual is more identifiable than certain other personally identifiable data elements that may be shared with others. For example, a student's Social Security Number, fingerprints, or other biometric data are unique to an individual. In contrast, other personally identifiable data elements, such as a ZIP code or date of birth may be shared by multiple students.[8]

In evaluating the sensitivity of individual personally identifiable data elements, the Governing Committee or the Data Subcommittee should take the potential for harm from an unauthorized or inadvertent disclosure into account. In this context, harm refers to any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII[9] (NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, p. 3-1, 2). In the case of a student, harm might include, for example, identity theft, discrimination, or emotional distress. The related harm to the organization responsible for the confidentiality breach could include loss of public confidence and public reputation, administrative burden of investigating the breach and ensuring necessary remedial steps are taken, and financial losses. To start the process of mitigating the disclosure of harmful information, personally identifiable data elements can be categorized by level of sensitivity (i.e., the likelihood of harm from an unauthorized disclosure)—perhaps as high, medium, and low. Note that any data elements identified as a PPRA-related variable should be categorized as a high-risk data element. After the risk level is established, consideration should be given to providing more protection and more restrictions on access for the data elements that are identified as highly sensitive. For example, these data elements might be stored apart from the rest of the student record in a more secure electronic environment, with access limited to "need to know" circumstances for only a subset of those with access to the system.

Summary

At this point the Governing Committee or its Data Subcommittee has inventoried and listed all personally identifiable data elements. The list includes descriptions of the following for each personally identifiable data element:

- Content/definition;
- Type of identifier—direct or indirect;
- PPRA related variable status;
- Specific use(s) and relevance;
- Accuracy;
- Timeliness for the intended use; and
- High, moderate, or low risk of harm from disclosure.

After a thorough review of the list, the Governing Committee should decide whether to retain all existing personally identifiable data elements and whether to go forward with the inclusion of any additional proposed personally identifiable data elements. The inventory of personally identifiable data should be updated each time new data elements are considered for inclusion in the student record data system.

[8] It is important to note, however, groups of the less sensitive identifiers can be combined to identify specific individuals. For example, researcher Latanya Sweeney used public anonymous data from the 1990 census to show that the combination of the five-digit residential ZIP code, gender, and exact date of birth could likely lead to the identification of 87 percent of the population in the United States (in 2005 testimony before the Pennsylvania House Select Committee on Information Security, House Resolution 351, Recommendations to Identify and Combat Privacy Problems in the Commonwealth).

[9] Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging).

Implement Internal Procedural Controls to Protect Personally Identifiable Information

The Fair Information Practice of *Security* calls for "Protecting personally identifiable information (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure." There are a variety of internal controls that can be employed to assist procedurally in the management of personally identifiable data.[10] The first set is a technical solution that involves assigning new unique student identifiers to protect students' PII in longitudinal electronic data systems. The second set focuses on procedures for workforce security to ensure that only authorized staff members are given access to personally identifiable student records. The third set combines aspects of the first two sets of controls in a role-based management approach that is intended to ensure that access to each student's education record is available on a "need-to know" basis. The fourth set involves operating rules for the conditions of use, such as rules concerning permissible uses and prohibiting unauthorized uses, procedures for protecting PII when it is in the possession of authorized users, and procedures for ensuring destruction of copies of records at the end of a period of authorized use. The fifth set of internal controls involves planning for possible data breaches by establishing procedures for reporting known or suspected breaches, analyzing the causes and impact of breaches, and notifying affected individuals.

Unique Student Identifiers and the Use of Linking Codes as Controls for Sensitive Information

In order to monitor the educational progress and experiences of individual students as they progress through the education system, a unique record identifier is needed to link each student's electronic record across grade levels and across schools, institutions, and related educational programs. Once attached to a student record, this identifier becomes part of that student's PII, as it must be unique to the student to be useful.

Each child already has a unique Social Security Number that could also be used to link to information in a student record system with information from education-related activities in other social service programs (e.g., Head Start or family services); thus, this might seem like the logical number to use as the student identifier in an electronic student record system in a K–12 or postsecondary setting. However, the Social Security Number should be treated as a sensitive piece of PII. In addition to being used to track a number of official electronic transactions, it is the single most misused piece of information by criminals perpetrating identity thefts. Using it on a day-to-day basis in an electronic student record system increases the possibility of a harmful disclosure that has ramifications beyond the student's education record. Instead, a separate unique student identifier that is distinct from the student's Social Security Number should be used on a day-to-day basis in an electronic record system.

The unique student identification number can be assigned at the school, district, or state level; however, care must be taken to ensure that within any record system each student has only one assigned identification number and that two students do not share the same identification number. If student records from separate schools within a district form a district-wide student record system, the student identification numbers should be assigned at the district level to ensure that each student in the district has a single unique identification number. Similarly, if all of the school districts in a state form a state-wide student record system, the student identification numbers should be assigned at the district level to ensure that each student in the state has a single unique identification number.

Each student's Social Security Number should be maintained as a data element in student record system because of the important role it plays when linkages are needed to other record systems (e.g., across states or across education levels within a state); however, consideration should be given to storing the student's Social Security Number in a separate secure location. To link the Social Security Number back to the rest of the student's record, a separate linking code must be assigned to each student's record. By attaching a linking code to each student's record, the student's Social Security Number, any other highly sensitive student information, and a copy of the linking code could

[10] There are also a number of electronic controls that can be implemented to assist in the management of personally identifiable data. They will be covered in a Technical Brief on electronic security.

be stored in a separate secure location apart from the student record that is used on a day-to-day basis. The linking code should not be based on a student's Social Security Number or other personal information, should not be used to identify a student's personal information, and should only be used for linking different components of individual student records.

Only a limited number of staff should have knowledge of the method used to generate the linking code. Further, only a limited number of authorized staff should have access to the secured sensitive information and should be permitted to use the linking code to combine two sets of records. Minimizing the number of times a student's Social Security Number and other sensitive data are accessed and limiting access to this information to a small set of authorized persons can help prevent unauthorized and inadvertent disclosures of the Social Security Numbers and other sensitive data.

Each student record system could use its own unique internal linking codes. Then, when record linkages are needed across different record systems (e.g., between states when a student moves or between a secondary school data system and a postsecondary institution's data system), each system can use its linking code to link the student record to the secured Social Security Number. The record(s) with Social Security Numbers attached should be safely transmitted to the administrator of the receiving record system and then stored in a secure environment until the records from the two separate systems are linked by matching the Social Security Number from the two record systems. Once the linked file is created and the data are checked, the Social Security Number should be removed from the combined file, and each student's linking code and Social Security Number is again securely stored.

Workforce Security and Authorization for Access to Personally Identifiable Information

Students and their parents provide the PII requested by the education system, with an expectation that the confidentiality of the information provided will be protected. To ensure that this expectation is fulfilled, administrators have a responsibility to confirm the trustworthiness of employees to whom sensitive student information is entrusted. This can be done through the use of security screenings, training, and binding confidentiality pledges.

PII carries a potential for misuse. As a result, it is advisable to require security screenings for staff members whose job responsibilities require them to have access to PII in student education records. The screening might include a background investigation using written, electronic, telephone, or personal contact to determine the suitability, eligibility, and qualifications of a staff member for employment.[11]

Administrators should establish job descriptions that delineate any uses of information that require access to PII from student education records Administrators should then provide annually recurring training to inform each employee with any job responsibilities that involve student education records of all legal and regulatory safeguard requirements that apply to the use and the design, development, operation, or maintenance of electronic student education records. The training should also cover all rules and procedures that are in place to ensure compliance with the safeguard requirements. Finally, the training should inform employees of the penalties that apply to the misuse of the information in student education records (NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, p. 4-1, 2, 3).

Following training, signed Affidavits of Nondisclosure can be used when providing access to confidential data to help ensure awareness of and compliance with all laws, regulations, rules, and procedural protections that apply. The affidavit should include the following:

- The time period approved for access;
- A pledge to protect the personally identifiable data in each student's education record;
- Citations to relevant laws, regulations, and rules;
- A description of penalties for violations; and
- An affirmation that the staff member has read and is aware of the documentation of the rules for handling and using student education records.

[11] The U.S. Department of Education requires all staff and contractors with access to personally identifiable information to undergo a security screening.

Requiring each authorized staff person to sign an Affidavit of Nondisclosure prior to being granted access to student education records fulfills the confidentiality pledge function.

Affidavits of Nondisclosure can be maintained to provide a record of the fact that each authorized staff member affirmed his or her commitment to protect the PII in student education records.

Once the affidavit is in place and access is granted, there are additional electronic mechanisms that can be used to protect the student education records and to monitor and record access and use for auditing and accounting purposes. Electronic security will be addressed in a separate Technical Brief.

Role Based Access to Student Record Data

As mentioned briefly in the discussion of job descriptions, the student information needed on a day-to-day basis varies across groups of employees depending on their roles in the education system. For example, an elementary school teacher is likely to need regular access to student data on attendance, grades, and student performance on various assessments, but not necessarily access to detailed information on the student's medical history or prior disciplinary actions. There are also likely to be differences in the amount of PII needed across levels of the education system. A program administrator for a district-wide program with a specific emphasis, such as science, math, or the arts, would need access to student education records including academic history and students' direct identifiers to organize placements into such programs. Meanwhile, an analyst in the district office who is responsible for generating aggregated reports of student performance for submission to the state education agency would need access to the performance results but not the direct identifiers for individual students.

Once defined, the job descriptions can be used to identify sets of data elements that are needed by groups of data users based on their roles in the education system. Then, rather than allowing each employee access to the full electronic student record or restricting access to needed data elements one user at a time, the database manager grants access to a set of data elements based on the data user's role.

This has been operationalized in statewide student record systems by the use of different access levels to protect personally identifiable and sensitive information in students' records. The Missouri Student Information System documentation, *Data Access and Management Policy* (pg. 6), offers a clear description of the goals in using access levels in the following statement: "All access levels are assigned in a way that maximizes usage by educators without risking inappropriate disclosure of personally identifiable information" http://www.dese.mo.gov/MOSIS/.

When a state uses access levels to control access to information in student records, the access level may control access to full records, with teachers, for example, being limited to students in their assigned classes, and principals having access to all student records in the school. The access level may also be used to control access to specific data elements (or fields) in the student records; finally, access levels can also be used to limit access to read only or to allow read and write access. In some instances, these three dimensions of control are used in combination (e.g., giving a teacher read and write access to a subset of data elements in the student records for the students enrolled in the teacher's class). As states develop systems for sharing student records across levels of the education system, the use of access levels can be expanded to encompass different roles in data use across levels.

Using Education Records

Once staff members have been authorized and granted access to student education records, they must abide by established rules and procedures for using the data—consistent with the terms agreed to in the Affidavit of Nondisclosure. Many of the security controls involved in using the data will be discussed in the Technical Brief on electronic security. However, there is an interface between access and use procedures and electronic security. Specifically, the Governance Committee should establish rules that identify where student records can be accessed. Within the school or office there may be restrictions placed on where staff members can access electronic student records. For example, access to the most sensitive information might be limited to specified secure locations, while access to less sensitive information might be allowed on a wider range of terminals. There may also be restrictions on whether access to student records is limited to the school or office, or whether remote access is permitted.

The use of access restrictions among authorized users will help protect the information in student records from authorized users who might be tempted to look at information they are not authorized to access (i.e., browsing) or from other unauthorized uses of student data. However, even among the staff members granted access to student records use of the information should be limited to permissible uses for the individual data elements, as established in the data inventory. To reinforce this, the Governance Committee should promulgate rules that prohibit browsing or unauthorized uses of information included in student education records.

The Governance Committee should also identify specific behaviors that could lead to inadvertent unauthorized access and establish rules prohibiting these actions. For example, authorized data users should not share a computer that houses identifiable student records with anyone not authorized to access those records, and they should not leave student record data with PII on an unattended computer screen. In a similar vein, if staff members are authorized to print hard copy of PII from student records, there should be rules that require secure storage of hard copy printouts or records (i.e., in a locked cabinet). In addition, if staff members are authorized to copy PII from student records to a CD-ROM or flash drive, there should be rules concerning security and protection of these electronic devices. There should also be record retention rules that govern the length of time a staff member may maintain a local electronic copy or subset of student record data and the length of time that a staff member can maintain hard copy of PII from student records. There should be complementary rules and procedures that govern the destruction of electronic and hard copy extracts of student information at the end of the approved access period.

Breaches of Personally Identifiable Information

Every privacy and data protection plan should include a response plan for the appropriate handling of a breach of PII if one occurs. The NIST 2010 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* includes a detailed discussion of how to handle data breaches. In particular, the Governance Committee should develop a clear description of what constitutes a breach. That description should be communicated to all staff members who are authorized to access PII in student records, along with a description of the immediate steps to take in the event a security breach occurs or is suspected. In particular, there should be a designated person in the management chain to notify in the event of known or suspected breaches involving PII. Contact information for the designated manager should be disseminated to all staff members, along with a list of the information that should be provided when reporting a known or suspected breach. The NIST 2010 Guide (Special Publication 800-122, pg. 5-1, 2) recommends that the report should include the following information:

- The name, job title, and contact information of the person reporting the incident;
- The name, job title, and contact information of the person who discovered the incident;
- Date and time the incident was discovered;
- Nature of the incident (e.g., system level electronic breach, an electronic breach of one computer or device, or a breach of paper extracts of records);
- Description of the information lost or compromised;

- Name of electronic system and possible interconnectivity with other systems;
- Storage medium from which information was lost or compromised;
- Controls in place to prevent unauthorized use of the lost or compromised information;
- Number of individuals potentially affected; and
- Whether law enforcement was contacted.

Known or suspected breaches of PII from student records should be reported as quickly as possible in an effort to mitigate any adverse events resulting from the breach. The Governance Committee should establish a time span for the reporting requirement (e.g., within one hour of discovery). The Governance Committee should also identify in advance how, when, and to whom notifications should be made (e.g., law enforcement, financial institutions, affected individuals, media, the public). Decisions concerning the breach notification should also be made as to the following:

- Whether breach notification to affected individuals is required;
- Timeliness of the notification;
- General content of the notification;
- Source of the notification (e.g., principal, superintendent, school board);
- Means of providing the notification (e.g., letter or public announcement);
- Who receives the notification (e.g., only affected individuals, general public);
- Remediation options to be provided, if any (e.g., a free copy of credit report, credit monitoring); and
- What corrective actions were taken and by whom.

When a breach occurs, the designated authority should conduct an analysis of the likelihood of exposure and potential harm to affected individuals (e.g., in the case of student records did the breach include Social Security Numbers and other information that could be used in identity theft, or was it limited to PII about the affected students' educational performance). This analysis will inform whether notification is required and the content of breach notification that is provided to affected individuals. There should also be an analysis of the circumstances that resulted in the breach so that the system or procedures can be modified as quickly as possible to avoid further breaches through the same mechanism.

Summary

At this point, the Governing Committee or its Data Subcommittee has reviewed job descriptions and identified the data elements needed for each position, identified authorization procedures for individual staff, and developed rules of access for authorized staff. The Governing Committee or a subcommittee has established a set of procedures to be used to assign unique student identification numbers for day-to-day use and has decided on a specific system architecture to be used in managing access to specific data elements. The Governing Committee or a subcommittee has also promulgated rules specifying the conditions of use for information in student education records, identifying permissible uses and prohibiting unauthorized uses; they have also established procedures for protecting PII when it is in the possession of authorized users and procedures for records disposition. Finally, the Governing Committee has also developed a plan of action to be executed in the event of a data breach.

Provide Public Notice of Education Record Systems

Providing public notice of the existence and use of a student education record system is another essential component of a privacy and data protection program. The Fair Information Practice of *Transparency* calls for "providing notice to the individual regarding the collection, use, dissemination, and maintenance of personally identifiable information" (NIST 2010 Special Publication 800-122, p. D-2, 3).

Annual Notifications

Consistent with the Fair Information Practice of transparency, FERPA and the related regulations require each educational agency or institution that receives funds from the U.S. Department of Education to provide all parents or eligible students[12] an annual notice of their rights with regards to the existence and use of student education records (20 U.S.C. § 1232g(e), 34 CFR 99.7). Insofar as some direct student identifiers are made available publicly as Directory information, FERPA also requires that parents are given an annual notice of the school or districts definition of student directory information, with the opportunity to opt out of the inclusion of their child's, or the eligible student's, directory information (20 U.S.C. § 1232g (e), 34 CFR § 99.7).

FERPA

Under FERPA and the related regulations, the institution, school, or the school district must provide parents with annual notification of their rights[13] and the procedures to use to inspect and review their children's education records and to seek amendment of inaccurate or misleading information in that record.[14] Furthermore, parents must be notified of the disclosures that are permissible under law without their consent,[15] and of the fact that they must consent to other disclosures of PII from their children's education records. Finally, the annual FERPA notice must describe the procedure for a parent to follow in filing a complaint of an alleged violation with the Family Policy Compliance Office (FPCO) in the U.S. Department of Education.

The annual notification does not have to be made individually to parents. Instead, it can be done through any of the following: local or student newspaper, calendar, student programs guide, rules handbook, or other reasonable means.

Directory

A school or district is also required to provide an annual Directory notice, if directory information is disclosed without consent. The school or district may choose to combine their annual FERPA notification with their annual Directory notice. Directory information includes information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed. The Directory notice must describe the specific types of information the school or district has designated as directory information, and the parent's right to opt out of disclosure of directory information. In the case of postsecondary institutions, these rights accrue to the student.

PPRA

The Pupil Protection Rights Act requires parental notification if a study to be conducted in a school includes any information or questions about the student or the student's family related to the eight identified sensitive topics: political affiliations or beliefs; religious practices, affiliations, or beliefs; mental and psychological problems; sex behavior or attitudes; illegal, anti-social, self-incriminating

[12] Eligible students are those age 18 and over or enrolled in postsecondary institutions.

[13] These rights transfer to the student when he or she turns 18 years of age or enters a postsecondary educational institution at any age ("eligible student").

[14] These requirements are consistent with The Fair Information Practices of Individual Participation and Redress, where redress involves "providing mechanisms for appropriate access, correction, and redress regarding the use of personally identifiable information."

[15] This must include a description of who is considered to be a school official and what is considered to be a legitimate educational interest.

and demeaning behavior; critical appraisals of family members; legally recognized privileged relationships; or income.[16]

If the study is funded by the U.S. Department of Education, schools and contractors must obtain written parental consent before minor students can be required to participate in the study. If the school received funds from the U.S. Department of Education, school districts are required to provide an annual schedule of the specific or approximate dates of all other surveys with a notification of the parents' right to request and review a copy of the survey before it is administered and to decide that their child will not participate, regardless of the survey's source of funding. Under this Act, parents must also be notified each year of their right to decide whether or not their child will participate in activities that make student's personal information available for marketing or other profit-making activities.[17] Parents must also be notified of their right to decide whether or not their child will participate in any non-emergency, invasive physical examination or screening that is scheduled in advance and administered by the school as a required condition of attendance but that is not necessary to protect the immediate health and safety of students.

Under PPRA, schools and contractors are also required to make instructional materials that will be used in any of the studies in which their children participate available for the parents' inspection. Planned surveys that include protected information must be made available for the parents' inspection prior to the administration of the survey.

Resources

The FPCO website includes more specific details and model FERPA notices to use at the school or district level (http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html) and at the postsecondary institution level (http://www2.ed.gov/policy/gen/guid/fpco/ferpa/ps-officials.html), as well as a model Directory notice (http://www2.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html) and a model PPRA notices for use by school districts (http://www2.ed.gov/policy/gen/guid/fpco/ppra/modelnotification.html).

Disclosure of Education Records

The Fair Information Practice of *Individual Participation* calls for "involving the individual in the process of using personally identifiable information and seeking individual consent for the collection, use, dissemination, and maintenance of personally identifiable information." Consistent with this practice, parent's rights to consent to disclosures of PII included in the student's education record must be described in the annual FERPA notice (FERPA, 20 U.S.C. § 1232g (e), 34 CFR §§ 99.7 and 99.30). To meet this requirement, a school must:

- Have a parent's consent prior to the disclosure of education records; and
- Ensure that the consent is signed and dated, specify the records that may be disclosed, state the purpose of the disclosure, and identify to whom the disclosure may be made.

The Fair Information Practice of *Purpose Specification* stresses the importance of "specifically articulating the authority that permits the collection of personally identifiable information and specifically articulating the purpose or purposes for which the personally identifiable information is intended to be used." The annual FERPA notice provides information about permissible uses of PII in education records. That is, FERPA allows educational agencies and institutions to non-consensually release education records to school officials and other designated entities with legitimate educational interests 20 U.S.C. § 1232g(b(1)(A), but the FERPA regulations require educational agencies or institutions that elect to disclose education records to the entities authorized in the Act to use the annual notice to specify the criteria used for identifying a school official and the definition of a legitimate educational interest. Specifically,

[16] See the earlier section *Identify All Personally Identifiable and Sensitive Information* for the complete text of the list as specified in law.

[17] This does not apply to information collected from students to support educational products or student services such as postsecondary education or military recruitment; book clubs, magazines, and programs providing access to low-cost literacy products; curriculum and instructional materials; tests and assessments used to provide information about students; the sale by students of products or services to raise funds for school-related or education-related activities; and student recognition programs.

under the FERPA regulations at 34 CFR § 99.31, a school may disclose PII from education records without consent when:

» The disclosure is to school officials who have been determined to have legitimate educational interests;

  - The disclosure is to other school officials, including teachers, within the agency or institution who have legitimate educational interests; a third-party contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services for which the agency or institution would otherwise use employees—as long as that third party's use and maintenance of education records is under the direct control of the agency or institution and is subject to the regulation requirements governing the use and redisclosure of PII from education records (34 CFR § 99.33(a)); and
  - An educational agency or institution uses reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests (34 CFR § 99.31(a)(1));

» The disclosure is to officials of another school, district, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer (34 CFR §§ 99.31(a)(2) and 99.34);

» The disclosure is to authorized representatives of the Comptroller General of the United States, the Attorney General of the United States, the Secretary of the Department of Education, or state and local educational authorities for the purpose of auditing or evaluating federal or state supported education programs or enforcing federal laws which relate to those programs (34 CFR §§ 99.31(a)(3) and 99.35);

» The disclosure is in connection with financial aid for which the student has applied or which the student has received if the information is necessary for such purposes as to determine eligibility, the amount, the conditions for the student to apply for or receive financial aid or enforce the terms and conditions of the aid (34 CFR § 99.31(a)(4));

» The disclosure is to organizations conducting studies for, or on behalf of, educational agencies or institutions for specified purposes related to predictive tests, student aid programs, or the improvement of instruction(34 CFR § 99.31(a)(6));

» The disclosure is to accrediting organizations to evaluate accreditation status (34 CFR § 99.31(a)(7));

» The disclosure is pursuant to a court order or a lawfully issued subpoena[18] (34 CFR § 99.31(a)(9));

» The disclosure is in connection with a health or safety emergency (34 CFR §§ 99.31(a)(10) and 99.36);

» The information disclosed has been appropriately designated as directory information by the school (34 CFR § 99.31(a)(11) and 99.37); and

» The disclosure is of de-identified student level data for the purposes of education research (34 CFR § 99.31(b)).

The SLDS Technical Brief on data sharing agreements will cover recommended terms for inclusion in agreements, along with a discussion of the specific uses permitted under legitimate educational interests, education research, and uses related to predictive tests, student aid programs, and the improvement of education.

Summary

A privacy and data protection program for student education records must include an array of rules and procedures for protecting PII held in the record system. It also must include a full set of public disclosures of the existence and uses of the information included in the data system, a description of all parents' or eligible students' rights to review and appeal the contents of an individual education record and of their rights and the procedures to appeal a violation.

[18] See 34 CFR § 99.31 for additional disclosures related to legal matters.

Accountability and Auditing

The Fair Information Practice of *Accounting and Auditing* calls for "Auditing for the actual use of personally identifiable information to demonstrate compliance with established privacy controls." This involves auditing the use of PII to demonstrate compliance with an organization's privacy and data protection plan, the privacy principles embodied in the Fair Information Practices, and all applicable privacy protection laws, regulations, and administrative requirements. The specific activities to be audited should be identified in the privacy and data protection plan. Many elements of a data security audit involve electronic security and will be discussed in the Brief on that topic. However, there are a several aspects of data stewardship that should be audited to confirm that required actions are taken to ensure the proper use and protection of PII in student education records. A failure to comply with any of the identified auditable elements of the privacy and data protection plan should be reported to appropriate officials for action.

Audit the Inventory of Personally Identifiable Information

The inventory of PII should include all current and proposed data elements (NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, pg. 2-2). The data manager should maintain records of the inventory of PII.

In the first data stewardship privacy audit, the inventory should be examined against the content of the existing longitudinal data system to determine whether the list of personally identifiable data elements maintained for students, teachers, and other staff members is complete.

Next, the audit should confirm that the inventory includes all of the required information for each data element. That is, for each data element, the inventory should include an indication of specific uses, whether it is a direct or an indirect identifier and the associated risk level and whether it involves any of the restricted topics identified in the Protection of Pupil Rights Act. Subsequent audits should identify updates to the record system that added new data elements and ensure that each new data element was added to the inventory and that all of the required information is included for each data element.

Audit of Data Quality and Integrity

FERPA (20 U.S.C. § 1232g (a) and the related regulations (34 CFR § 99) establish the right of a parent to inspect and review his or her child's (or in the case of an eligible student his or her own) education record for accuracy. The data manager should develop procedures that result in data that are up to date and complete and that accurately reflect the students' educational experiences. Periodic audits of data quality can support data quality by either substantiating the quality of individual data elements or identifying inaccuracies for correction. Periodic quality audits should be built into the data collection, reporting, and release cycle.

The NCES-sponsored National Forum on Education Statistics published the 2004 report *Forum Guide to Building a Culture of Data Quality* to assist schools and school districts in the development of procedures to improve the accuracy, utility, timeliness, and security of data in education data systems. The Forum web site also provides lesson plans as part of the *Forum Curriculum for Improving Education Data (*http://nces.ed.gov/pubs2007/curriculum/index.asp). The curriculum is designed for use in schools and school districts to support the production of "high-quality education data," with the goal of presenting the concepts and skills needed to improve data quality. One of the lessons included in the curriculum is *Validating and Auditing Data* (http://nces.ed.gov/pubs2007/curriculum/ls_validating.asp).

The goals of the curriculum on data validation and audits include describing the steps required to validate data, describing the purpose of a data audit, and identifying the steps included in a data audit in order to outline a plan for a data audit. The data validation involves data entry, checking for errors, confirming errors are real and not outliers, identifying each place the incorrect data element is stored in the data system, and providing corrections to the data entry staff.[19]

[19] While these data validation activities have broader utility than those involved with privacy, ensuring the accuracy and validity of data maintained in an education record system is consistent with the FERPA requirement that parents have the right to review the accuracy of their children's information.

The audit confirms the accuracy of the data that are released for use by the school and district staff and by the public. To conduct a successful audit of data accuracy, the first step is to identify the released data (e.g., printed reports, tables published on the web, online table generator), and then the data should be analyzed, looking especially for data anomalies. If suspected data anomalies are identified, the audit next focuses on whether they represent real change or whether they are the result of an error. If an error is identified, the source of the error should be investigated (e.g., data recording error, transposed number, data entry error), and the needed correction should be identified. Related procedures are reviewed to identify any needed changes. Staff who contributed to the error should be notified and provided instruction needed to avoid repeating the error. Finally, notice of the changed data should be provided to all data users.

Audits of Internal Controls used to Protect Personally Identifiable Information

Unique Student Identifiers

Longitudinal student record data requires a unique record identifier for each student in a data system. That unique identifier is needed to link each student's electronic record across grade levels and across schools, institutions, and related educational programs. Once attached to a student record, this identifier becomes part of that student's PII, as it must be unique to the student to be useful. Thus, the audit of internal controls should start with an examination of the process used to assign unique student identification numbers. The first question is whether unique identification numbers other than the students' Social Security Numbers are in place for use in day-to-day operations. If so, the next task is to confirm that the student identification numbers are not based on the students' Social Security Numbers; that the students' Social Security Numbers are securely stored apart from the student records that are used daily; that a linking code exists to be used to link a student's record to that student's Social Security Number when the need arises (e.g., the student transfers out of state or transitions to postsecondary education); and that the method for generating the linking key is closely protected, with knowledge limited to a small number of staff positions.

The student identification numbers should be audited to ensure that each student has only one identification number. This can be done electronically by searching for matching data on the combination of name, age, grade, sex, and race/ethnicity. If matches occur, the student records should be examined further to confirm that there are not multiple records for an individual student. These matches should include options for multiple spellings of names and for the use of initials in addition to, or in place of, the first name. If any students are found with multiple student identification numbers, the records should be consolidated into one record using only one of the identification numbers for that student and the duplicate records should be deleted.

Conversely, the student identification numbers should be examined to confirm that the same number is not being used for multiple students. This can be done by electronically searching for exact matches on two or more identification numbers. If matches occur, the associated the records should be examined to confirm whether the records are for different students or whether there are two records for the same student (perhaps with a full first name on one record and initials in place of the first name of the second record). If one identification number has been assigned to two or more students, each student should be given a new unique identification number. If one identification number is being used for two different records for the same student, the two records should be reconciled and combined under the existing student identification number.

Workforce Security and Permitted Access to Personally Identifiable Information

To ensure that the requirements of FERPA are met and that PII is protected, administrators have a responsibility to protect access to that information and to confirm the trustworthiness of employees to whom sensitive student information is entrusted. An audit of workforce security should start with a review of job descriptions to ensure that the need for access to PII is clearly specified. Then once the positions with a need for access are identified, the audit should review the list of staff members in those positions against the documentation for completed background investigations to ensure

that each staff member with access to personally identifiable and sensitive student information has successfully passed a background check. The audit should review the same list of staff members against the list of staff who completed the required privacy and data protection training and the file of signed confidentiality pledges (i.e., affidavits of nondisclosure) to ensure that each staff member with access to personally identifiable and sensitive student information is aware of the relevant laws, regulations, and rules and has agreed to uphold them to protect student information.

The data manager should also have records documenting the authorized level of access for each data user granted access to any personally identifiable student information. There should be an access control system in place, and an audit should be conducted to ensure that each data user's level of access is in line with that person's current job description. If discrepancies are found, the level of access should be corrected, or a justification for the deviation from established access levels should be documented. In addition, the current levels of access should be compared to the approved levels of access. If discrepancies are found, the level of access should be corrected, or a justification should be provided and the data user's access level should be corrected in the data manager's records.

Summary

A privacy and data protection program for student education records must include a set of checks and balances to ensure that the necessary rules and procedures are in place and that they are being fully implemented. This is best done through a formal periodic audit of the various processes involved in the processing and usage of personally identifiable student information. Starting with the careful identification of the personally identifiable and sensitive data elements, continuing through the data processing and reporting to the day-to-day usage of student information. The audit starts by identifying the relevant governing rules and procedures, examines the records for deviations from the rules and procedures, and ensures that needed corrections are implemented. Where possible, the audit should identify the factors that contributed to the problems identified, examine the related processes, and make suggestions for procedural changes that might reduce the number of similar problems in future audits.

References

American Statistical Association, Committee on Privacy and Confidentiality, *Key Terms/ Definitions in Privacy and Confidentiality.* Alexandria, VA: Retrieved from http://www.amstat.org/committees/pc/keyterms.html on 6/17/2010.

Code of Federal Regulations, Title 34—Education, Part 99. *Family Educational and Privacy Rights,* (34CFR99). Washington, DC: GPO Access e-CFR. Retrieved from http://ecfr.gpoaccess.gov/cgi/t/text/ext-idx?c=ecfr&sid=44d350c26fb9cba4a156bf805f297c9e&tpl=/ecfrbrowse/Title34/34cfr99_main_02.tpl on 9/10/2010.

The Federal Chief Information Officers Council (2008). *Federal Enterprise Architecture Security and Privacy Profile, Version 2.* Washington, DC: Federal Enterprise Architecture Program Management Office, Retrieved from http://www.cio.gov/Documents/Security_and_Privacy_Profile_v2.pdf on 6/17/2010.

National Forum on Education Statistic (2004). *Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies,* (NCES 2004-330). Washington, DC: Retrieved from http://nces.ed.gov/pubs2004/2004330.pdf on 6/17/2010.

National Forum on Education Statistic (2004). *Forum Guide to Building a Culture of Quality Data: A School & District Resource,* (NFES 2005-801). Washington, DC: Retrieved from http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2005801 on 6/17/2010.

McCallister, E., Grance, T., and Scarfone, K. (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology* (NIST Special Publication 800-122). National Institute of Standards and Technology, U.S. Department of Commerce. Washington, DC: Retrieved from http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf on 5/4/2010.

Sweeney, Latanya. (2005). *Recommendations to Identify and Combat Privacy Problems in the Commonwealth.* Testimony on House Resolution 351, Pennsylvania House Select Committee on Information Security.

U.S. Code, Title 20—Education, Chapter 31—General Provisions Concerning Education, Subchapter III—General Requirements and Conditions Concerning Operation and Administration of Education Programs: General Authority of Secretary, Part 4—Records, Privacy, Limitation on Withholding Federal funds, Section 1232g. *Family Educational and Privacy Rights,* (20USC1232g). Washington, DC: GPO Access. Retrieved from http://frwebgate4.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=799486197532+0+1+0&WAISaction=retrieve on 9/10/2010.

U.S. Code, Title 20—Education, Chapter 70—Strengthening and Improvement of Elementary and Secondary Schools, Subchapter I—Improving the Academic Achievement of the Disadvantaged, Part A—Improving Basic Programs Operated by Local Educational Agencies, Subpart 1—Basic Program Requirements, Section 6311. *State Plans,* (20USC6311). Washington, DC: GPO Access. Retrieved from http://frwebgate2.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=bULwJH/21/1/0&WAISaction=retrieve on 9/10/2010.

U.S. Code, Title 20—Education, Chapter 76—Education Research, Statistics, Evaluation, Information, and Dissemination, Subchapter I—Education Sciences Reform, Section 9547. *Cooperative Education Statistics Systems,* (20USC9547). Washington, DC: GPO Access. Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc20.wais&start=10271732&SIZE=977&TYPE=TEXT on 9/10/2010.

U.S. Code, Title 20—Education, Chapter 76—Education Research, Statistics, Evaluation, Information, and Dissemination, Subchapter II—Educational Technical Assistance, Section 9607. *Grant Program for Statewide, Longitudinal Data Systems,* (20USC9607). Washington, DC: GPO Access. Retrieved from http://frwebgate3.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=FKr6BA/0/1/0&WAISaction=retrieve on 9/10/2010.

U.S. Department of Commerce, National Institute of Standards and Technology (2010). *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* (SP 800-122). Gaithersburg, MD.

U.S. Department of Health and Human Services, Report of the HEW Secretary's Advisory Committee on Automated Personal Data Systems (1973). *Records, Computers and the Rights of Citizens,* Washington, DC: Retrieved from http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm on 5/11/2010.

U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum (2008). *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security,* Washington, DC: Retrieved from http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf on 6/17/2010.

U.S. Public Law, 110-69, America Competes Act, Title VI—Education, Section 6401. Washington, DC: GPO Access. Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ069.110 on 9/10/2010.

U.S. Public Law, 111-5, American Recovery and Reinvestment Act, Title VIII—Education, Institute of Education Sciences. Washington, DC: GPO Access. Retrieved from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_public_laws&docid=f:publ005.111 on 9/10/2010.