Recommendations and Funding Proposal to Further Improve or Enact High-Quality Practices and Supports to Safeguard Student Personally Identifiable Information

Prepared for the Utah State Office of Education

by

ESP Solutions Group, Inc.

Recommendations for Action

December 4, 2015

Glynn Ligon, Ph.D.

Steven King

Barbara Clements, Ph.D.

Executive Summary

The Utah State Office of Education (USOE) satisfies a public need by collecting data about students to support decision making, to respond to federal and State mandates, and to provide necessary information to manage the schools and improve instruction. Best practices in recent years have proven that collecting individual student records is more cost-effective and efficient than aggregate data to satisfy these purposes and to ensure quality data. Local education agencies (LEAs) collect individual student data to manage instruction and populate the many information systems that manage their schools. Incumbent upon both LEAs and USOE is the requirement to protect the confidentiality of personally identifiable information (PII) within their information systems and all published reports.

The Family Educational Rights and Privacy Act protects the right of parents and students to access and manage personal data. Many individual states and LEAs are designating a Chief Privacy Officer (CPO) to oversee the stewardship of PII and support parents, students, and LEAs in the proper access, use, and maintenance of PII.

To fulfill the requirements of U.C.A. 1953 § 53A-1-711, recommendations and a funding proposal were developed to inform legislation regarding PII. This document provides an overview of the issues related to this task.

The expectation for future legislation and guidance from USOE is to provide guardrails within which educators can safely operate with personally identifiable student data. Knowing the guidance provided should create a context within which educators will work with confidence rather than concern about unclear or unknown requirements and penalties.

The key issues from U.C.A. 1953 § 53A-1-711 are organized in this document under seven questions that drive the specific recommendations. Some questions can be addressed with simple answers. Others require very complex processes to be designed, adopted, and maintained.

1. How can an LEA and USOE better maintain, secure, and safeguard student data including using industry best practices?

2. How can an LEA and USOE provide disclosures to parents and students on how student data will be collected, maintained, and used?

3. How should directory information be defined (i.e., by USOE or the LEA) and managed?

4. How does an LEA or USOE allow a student to expunge the student's data?

5. How does an LEA or USOE ensure a contract with a third-party service provider provides for restrictions on the use of student data; dates for destruction of student data; no secondary uses of student data (e.g., sales, marketing, or advertising), limiting use of student data only to services to the education entity; and using industry best practices to maintain, secure, and safeguard the student data?

6. What should be the penalties for the unauthorized release of or failing to maintain, secure, and safeguard student data?

7. What funding is needed at USOE to support LEAs and to protect the rights and privacy of students?

The major recommendations can be summarized into three high-level categories.

1. Development of a Data Governance Plan for USOE and each LEA

    a. Three Advisory Groups:
        i. Policy Advisory Group
        ii. USOE Advisory Group
        iii. Users Advisory Group

    b. Metadata Dictionary: Defines and discloses all data collected, stored, and reported with the mandate for doing so; published on a public website. Data elements categorized as:
        i. Necessary or Required;
        ii. Optional; or
        iii. Not Allowed.

    c. Security Plan: Confidential plan for maintaining system security

    d. Institutional Review Board: Reviews external research requests

    e. Three-Tier Database: Public masked aggregate statistics, de-identified research database, and secure official USOE longitudinal database

2. Contents: Exchanging data with other agencies, de-identification of data within systems, responding to breaches or complaints related to violations of PII, determining retention and destruction timelines for data, gathering public comments to influence policy and practice, implementing best practices, expunging data, defining roles for key personnel, and recommending to the Policy Advisory Group data elements not allowed to be collected or reported. Creation of data management roles at each LEA with specific responsibilities related to stewardship of personally identifiable information

    a. Chief Privacy Officer: The ultimate authority in the LEA for policy and practice related to the protection and management of PII.

    b. Records Manager: The primary contact for USOE for all matters related to data collection and reporting.

c. Privacy Monitor: The person overseeing the processes for publishing, monitoring, and implementing PII procedures.

d. Privacy Lead: The team leader for security, software systems compliance, and other technical issues.

3. Funding for:

- Training, support, and auditing of LEAs;

- Publishing of metadata dictionaries to document and disclose what is collected and reported;

- Development of security plans for USOE and LEAs; and

- Development of materials based upon best practices

Question 1: How can an LEA and USOE better maintain, secure, and safeguard student data including using industry best practices?

Personally identifiable information must be protected following FERPA mandates. Agencies and institutions must use appropriate physical, technical, administrative, and operational controls to limit access to only those school officials (i.e., staff) with a legitimate need to know (e.g., role-based security features). Policies must exist to ensure that controls are in place. Section 99.31

Data are collected in different ways by the different LEAs and schools, and by USOE.

Some data collection methods are more efficient than others today (e.g., direct extraction-transformation-loading student data from an LEA's student information system to the USOE's operational data store compared to outdated paper submission forms). Transitioning to those can require an initial dollar investment and training. The benefits are typically improved timeliness and data quality. The objective is ultimately to collect all data into the same format and have them all meet the required rules for quality. Data collections by USOE from all LEAs have been standardized for individual collections, but still vary across collections.

Data collection methods by individual LEAs reflect their local size, level of automation, adoption of specific software applications, and local preferences. The training, skills, and job title of the persons handling and reporting the data at the local level vary.

The timeliness and quality of the data reported can be measured for each LEA. LEAs requiring support to improve can be identified. Providing support, training, and documentation for LEA staff are the basics for best practices. Staff turnover will always ensure a constant need for training and support.

There is not always a Chief Privacy Officer designated at the LEA level. The designation of Chief Privacy Officer (CPO) is becoming more common. CPO is more often a role rather than a full-time position in an LEA. Support, training, and a clear definition of responsibilities provide the foundation for whomever is designated in that role. The CPO typically functions at an executive level. Therefore, two additional roles are required for implementation success. A Privacy Monitor role is needed to ensure that reports and public documents do not disclose personally identifiable information. A Privacy Lead role is required to ensure that all data systems are secure and protect personally identifiable information. Depending upon the size of an education agency, these roles may be performed by one or more persons.

The protocols for managing data vary across the LEAs. This raises the question of whether or not each LEA is following best practices for data governance and the processes for collecting, storing, securing, accessing, sharing, and destroying data.

These protocols continue to grow more technical and complex. However, they remain within a policy context. A standard data governance structure supported by basic tools and processes can be customized to each LEA's size and context.

LEAs typically do not have the local resources to stay up-to-date with best practices for collecting, storing, securing, accessing, sharing, and destroying data. Continual training and support are required from USOE.

Implementation of privacy and security processes varies across LEAs. This raises the question of whether or not each LEA is following best practices for data governance and the processes for timelines, resources, transparency, accountability, notifications, and disclosure.

Standard data governance guidance is needed by all LEAs and needs to be continually updated.

USOE has a longitudinal database with personally identifiable student data accessible by authorized and authenticated staff for internal purposes. USOE creates public statistical reports with masked statistics, which protect the identities of individual students. USOE creates de-identified research data files as needed for research purposes.

The science and psychometrics of de-identification of databases and the suppression of statistics in public reports has become very complex as computer analytics have progressed. Agencies face a paradox. If they de-identify a database too much, then they can no longer perform the analyses they desire to calculate official statistics or to answer crucial decision questions. A three-tier solution has emerged as best practice.

- Tier 1: Identified individual data for internal, official use

- Tier 2: De-identified individual data for research

- Tier 3: Suppressed/masked statistical data for public use

Recommendations:

1. USOE should develop and maintain a Data Access and Management Plan for Data Governance, e.g., Data Governance Plan. The Data Governance Plan should provide for three levels of oversight and guidance.

    a. **Policy Advisory Group**—This group should have members representing the State Board of Education, State Legislature, Utah State Office of Education, local education agencies, and other policy entities as identified by the (State Superintendent of Public Instruction or State Board of Education). The Policy Advisory Group would perform duties such as oversee legislation, adopt common policies across State agencies, and adopt recommendations to the Legislature such as a list of data elements not allowed to be reported to USOE or collected by LEAs. The Policy Advisory Group would review and approve the Data Governance Plan prepared and maintained by USOE.

    b. **USOE Advisory Group**—This group should have members from program offices and managers within USOE. The USOE Advisory Group would perform duties such as review and approve new data collections by program offices, adopt standard definitions of data elements, review and approve security plans, and coordinate the calendars for data collection and reporting activities. The USOE Advisory Group would prepare and maintain USOE's Data Governance Plan, and recommend it to the Policy Advisory Group for approval.

c. **Users Advisory Group**—This group should have members from stakeholder groups such as LEAs and others who report and use data. The Users Advisory Group would advise the USOE Advisory Group and the Policy Advisory Group on issues such as the practical aspects of their proposed actions, suggestions for training and support, and feedback on the functions of information systems including privacy and security issues. The Users Advisory Group would review and comment on the template for an LEA Data Governance Plan as prepared by USOE, and make recommendations for related training and support activites.

2. USOE's Data Governance Plan, among other topics necessary for guiding and managing data and information systems, should address these issues: exchanging data with other agencies, de-identification of data within systems, responding to breaches or complaints related to violations of PII, determining retention and destruction timelines for data, gathering public comments to influence policy and practice, implementing best practices, expunging data, defining roles for key personnel, and recommending to the Policy Advisory Group data elements not allowed to be collected or reported.

3. USOE should develop for LEAs a template for a Data Governance Plan. Each LEA should adopt and implement a Data Governance Plan, which should be submitted annually to the USOE CPO for review and approval.

4. USOE should provide technical assistance, training, and support for best practices in data governance.

5. USOE should develop a Data Security Plan. The Data Security Plan should encompass all internal systems and systems provided and maintained by contractors.

6. USOE should develop for LEAs a template for a Data Security Plan. Each LEA should adopt and implement a Data Security Plan, which should be submitted annually to the USOE CPO for review and approval.

7. USOE should provide technical assistance, training, and support for best practices in data security.

8. USOE should implement the three-tiered database approach to protect PII and to ensure appropriate access to data for analysis and reporting.

9. USOE should provide technical assistance to LEAs to implement the same three-tiered database approach as appropriate.

Question 2: How can an LEA and USOE provide disclosures to parents and students on how student data will be collected, maintained, and used? How should directory information be defined (i.e., by USOE or the LEA) and managed?

FERPA requires that parents and eligible students annually be informed about their rights under the act including the right to inspect and review what is contained in the student's record (Sections 99.10-12) and the restrictions on release of the student's data without parental permission. (Sections 99.30-39) Education agencies may identify directory information that can be released without parental permission for particular purposes and include this information in the annual public notification. (Section 99.7, and 99.37) However, FERPA does not specify that parents and students must be informed about what data will be collected and their use. Annually at registration and continually on an agency website, the LEA should provide a statement to each parent and eligible student.

> *Directory information* means information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (*e.g.,* undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors, and awards received; and the most recent educational agency or institution attended. (Authority: 20 U.S.C. 1232g(a)(5)(A))

Defining a student record is important for this discussion. FERPA provides this definition.

<u>Education Records</u>

>   (a) The term means those records that are:

>>   (1) Directly related to a student; and

>>   (2) Maintained by an educational agency or institution or by a party acting for the agency or institution.

>   (b) The term does not include:

>>   (1) Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.

>>   (2) Records of the law enforcement unit of an educational agency or institution, subject to the provisions of §99.8.

>>   (3)(i) Records relating to an individual who is employed by an educational agency or institution, that:

>>>   (A) Are made and maintained in the normal course of business;

(B) Relate exclusively to the individual in that individual's capacity as an employee; and

(C) Are not available for use for any other purpose.

(ii) Records relating to an individual in attendance at the agency or institution who is employed as a result of his or her status as a student are education records and not excepted under paragraph (b)(3)(i) of this definition.

(4) Records on a student who is 18 years of age or older, or is attending an institution of postsecondary education, that are:

(i) Made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity;

(ii) Made, maintained, or used only in connection with treatment of the student; and

(iii) Disclosed only to individuals providing the treatment. For the purpose of this definition, "treatment" does not include remedial educational activities or activities that are part of the program of instruction at the agency or institution; and

(5) Records created or received by an educational agency or institution after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student.

(6) Grades on peer-graded papers before they are collected and recorded by a teacher.

(Authority: 20 U.S.C. 1232g(a)(4))

There is a "data disconnect" on what's collected, shared, and secured across LEAs, e.g., SSN. (LEAs have disparate policies and procedures governing the data they collect, how the data are shared with other entities, and how those data are protected.)

Most of the data collected from LEAs by USOE are required by the federal government. Many of those data elements are also used by USOE for school funding formulas and basic demographic statistical reporting. These data elements are standardized across LEAs in their periodicities and definitions. How these data are shared between the LEAs and USOE is also standardized and secure. LEAs must collect data for the Office for Civil Rights and individual federal and private grants they procure.

LEAs determine the "functional" data elements they desire such as immunizations, addresses, and classroom numbers to manage and align their data. LEAs procure their own enterprise systems for human resources, transportation, and finance, which at times determine the standards or vendors they

use for student systems. LEAs' choices of their student information system software determines a significant portion of how they collect student data.

LEAs determine their own interagency data sharing arrangements; how data are accessed for research and freedom of information requests; and how data are reported to the public.

There is no statewide standard process for protecting student data either for confidentiality of personally identifiable information or security of information systems.

In order to ensure that notices to the public and parents are up-to-date, these notices, such as the posting of the metadata dictionary and the LEAs' list of data collections, should be on a public website.

A **metadata dictionary** is defined as a reference guide defining an agency's data collections, repositories, and outputs (i.e., reports, web resources, and other manner of providing access to data). Related to each of these are the offices and persons responsible for them, the periodicities for their collection and reporting, and the definitions for individual data elements and codes. The metadata dictionary does not contain actual data, but the documentation for how to properly interpret and use the data.

Generally, there are three categories defined for how states specify what data elements may or may not be collected about individual students. These were also vetted through discussions throughout Utah during the development of Version 3 of House Bill 68.

1. **Necessary and Required**

    a. Necessary to conduct the activities of the school and district

        Each school and district determines the data elements necessary to conduct their activities including enroll students, deliver instruction, assign students to classes, and maintain academic records. Data elements might include immunization records, name, birthdate, class assignment performance scores, and attendance. Necessary data would include directory information, which parents would have the right to withhold from public release.

    b. Required by State or federal mandate

        State and federal mandates require collection and reporting (in aggregate form at a minimum) of data elements such as gender, race/ethnicity, and graduation status.

2. **Optional** by parental or student permission for eligibility and participation in programs and services

        In order to participate in special programs or receive services (e.g., free or reduced-price meals, English as a Second Language instruction, or special education), parents or students must opt to provide specific data elements such as family income, migratory status, or handicapping condition.

3. **Not Allowed**
    a. Not allowed to be reported by the LEA to the state for storage in a longitudinal data system and reporting

        Certain data elements may be specified as not allowed to be reported by the LEA to the state education agency for access in their longitudinal data system or to be reported in their public statistics.

    b. Not allowed to be collected systematically by the LEA

        Certain data elements may be specified as not allowed to be systematically collected by the LEA about students to be kept in their information systems.

Knowing the mandate and uses for data collected about students is fundamental to data governance. Understanding the mandate and uses is required to determine when a parent or student has the right to choose whether or not to provide the data to the school or whether or not the data may be disclosed to another party.

Managing PII at the LEA level requires multiple roles. These roles may be performed by one or more persons depending upon the size and organizational structure of the LEA.

- **Chief Privacy Officer**: The ultimate authority in the LEA for policy and practice related to the protection and management of PII

- **Records Manager**: The primary contact for USOE for all matters related to data collection and reporting

- **Privacy Monitor**: The person overseeing the processes for publishing, monitoring, and implementing PII procedures

- **Privacy Lead**: The team leader for security, software systems compliance, and other technical issues

Recommendations:

1. USOE should publish on its website a statement that describes how student data are collected, maintained, and used. This website should provide continually updated information about:

    a. USOE's Data Governance Plan;
    b. USOE's metadata dictionary including data collected, maintained, and reported;
    c. Data elements approved as necessary or required, optional, or not allowed;
    d. Processes for applying for access to data for research and evaluation purposes; and
    e. Other policies and procedures related to the management of student data.

2. USOE should provide to LEAs technical assistance and guidance for best practices for disclosing to parents and students how student data are collected, maintained, and used; including the maintenance of a local website such as described for USOE.

3. Each LEA should provide to USOE a current list of the person or persons performing each of these roles: Chief Privacy Officer, Records Manager, Privacy Monitor, and Privacy Lead.

4. Each LEA should continue to define directory information (e.g., the specific data elements that will be considered directory information) and inform parents and students at registration annually and continuously on a public website. USOE should audit these processes to ensure they are adequate and reflect best practices.

5. The data governance process described in Question 1 should guide these activities.

6. The USOE Advisory Group should recommend to the Policy Advisory Group annually the metadata dictionary containing the data elements designated as Necessary or Required, Optional, and Not Allowed as determined by the USOE Advisory Group.

7. The Policy Advisory Group defined should recommend the list of data elements specified as Not Allowed to be collected or reported. These should be recommended to the Legislature annually for adoption. In the event that the U.S. Office of Management and Budget approves collection of federally mandated data elements that are currently on Utah's list of those Not Allowed without sufficient lead time for the Legislature to act upon collecting and/or reporting those data elements, then the Policy Advisory Group should be empowered to authorize those elements to be collected and/or reported as necessary to comply with the federal mandate until the Legislature can take action.

Question 3: What is the process for an LEA and USOE to release student data to an education entity, a government entity, a person, or a private third party (within or outside the State)?

FERPA includes restrictions on the release of data without parental permission, including release to educators/education institutions, health or safety institutions, and juvenile justice systems. Recordkeeping requirements are specified in detail in Sections 99.30-39.

A Data Access and Management Policy, Data Governance Plan, should specify these processes and the data governance process to oversee them.

Requests for student data under the Government Record Access Management Act (GRAMA) or for research purposes demand time and resources of USOE and the LEAs. USOE has a single webpage for requestors to start their process. For non-confidential data, http://www.schools.utah.gov/data/Data-Request.aspx. For confidential data, the research application is http://www.schools.utah.gov/data/Data-Request/ResearcherProposal.aspx. LEAs have various processes for requestors to follow. Having to understand these different processes can lead to researchers collecting data that may already be available within the LEA's data systems, thus imposing additional burden on the schools.

An Institutional Review Board (IRB) is a committee established to review and approve research involving human subjects. The purpose of the IRB is to ensure that all human subject research be conducted in accordance with all federal, institutional, and ethical guidelines. This includes protection of personally identifiable information.

Recommendations:

1. USOE should adopt a Data Governance Plan that is in compliance with FERPA Sections 99.30-39. The plan should provide for processes that are consistent with Utah law for the release of student data to an education entity, a government entity, a person, or a private third party (within or outside the State).

2. USOE should provide technical assistance and support to LEAs to ensure that each has a Data Governance Plan that is in compliance with FERPA Sections 99.30-39. These plans should provide for processes that are consistent with Utah law for the release of student data to an education entity, a government entity, a person, or a private third party (within or outside the State).

3. The USOE Privacy Auditor should ensure that each LEA's Data Governance Plan complies with the requirements for release of student data.

4. USOE should adopt a process for review by an Institutional Review Board for all research conducted using student data.

5. USOE's CPO should ensure that checks are in place to monitor compliance with the requirements for review by an Institutional Review Board.

6. LEAs should be required to implement equivalent processes for review of all research conducted using their student data.

7. The USOE Privacy Auditor should ensure that each LEA's Data Governance Plan complies with the requirements for review by an Institutional Review Board.

Question 4: How does an LEA or USOE allow a student to expunge the student's data?

FERPA requires that parents or eligible students be given the right to review the student's record to see if the record contains information that is inaccurate, misleading, or in violation of the student's rights of privacy, in which case he or she may ask the educational agency or institution to amend the record. The parent or student may be given a hearing and the education institution may decide whether or not to amend the record. (Sections 99.20-22)

A Data Access and Management Policy should specify these processes and the data governance process to oversee them. The definition of "expunge" should be clearly defined to ensure that it is consistent with other Utah laws. Generally, expungement is the process to "remove from general review" the records pertaining to a case. In some jurisdictions, the data may not be completely deleted and may still be available to law enforcement or others with a legal authority. The burden upon USOE and LEAs for expunging data under differing definitions must be considered.

Recommendations:

1. USOE should adopt a Data Governance Plan that is in compliance with FERPA Sections 99.20-22. The plan should provide for processes that are consistent with Utah law for expunging student data. The legal parent or guardian, or student 18 years old or older may request in writing data be expunged or amended if those data are inaccurate, misleading, or violate the student's rights to privacy. A request may also be made to expunge data that are not defined as required and permanent in the Data Governance Plan.

2. USOE's CPO should ensure that checks are in place to monitor compliance with the requirements and processes for expunging student data.

3. USOE should provide technical assistance and support to LEAs to ensure that each has a Data Governance Plan that is in compliance with FERPA Sections 99.20-22. These plans should provide for processes that are consistent with Utah law for expunging student data.

4. The USOE Privacy Auditor should ensure that each LEA's Data Governance Plan complies with the requirements and processes for expunging student data.

Question 5: How does an LEA or USOE ensure a contract with a third-party service provider provides for restrictions on the use of student data; dates for destruction of student data; no secondary uses of student data (e.g., sales, marketing, or advertising), limiting use of student data only to services to the education entity; and using industry best practices to maintain, secure, and safeguard the student data?

FERPA restricts an educational agency or institution from disclosing personally identifiable information from an education record only on the condition that the party to whom the information is disclosed will not disclose the information to any other party without the prior consent of the parent or eligible student. (Section 99.33) Organizations receiving personally identifiable data must be required to maintain the confidentiality and privacy of the data, use the data only for stated purposes and as long as agreed upon, and destroy the data when no longer needed. The disclosing organization must ensure that these (and other specified requirements) are met. (Section 99.35)

A Data Access and Management Policy should specify these processes and the data governance process to oversee them.

Recommendations:

1. USOE should develop standard language to be included in each contract with a third-party provider that provides for restrictions on the use of student data; dates for destruction of student data; no secondary uses of student data (e.g., sales, marketing, or advertising), limiting use of student data only to services to the education entity; and using industry best practices to maintain, secure, and safeguard the student data.

2. USOE's CPO should ensure that checks are in place to monitor compliance at USOE.

3. USOE should develop standard language to be included in each LEA's Data Governance Plan to ensure a contract with a third-party service provider provides for restrictions on the use of student data; dates for destruction of student data; no secondary uses of student data (e.g., sales, marketing, or advertising), limiting use of student data only to services to the education entity; and using industry best practices to maintain, secure, and safeguard the student data.

4. The USOE Privacy Auditor should ensure that each LEA's Data Governance Plan complies.

Question 6: What should be the penalties for the unauthorized release of or failing to maintain, secure, and safeguard student data?

FERPA contains a set of provisions for reporting infractions to the Family Policy Compliance Office of the U.S. Department of Education. (Sections 99.60-67) Penalties include restrictions of access to data by the offender for five years. State and local penalties may be identified in law or regulations such as fines or personnel restrictions if desired.

If Utah followed the model of the Health Insurance Portability and Accountability Act (HIPAA), then fines and jail time would be scaled based upon the state of mind of the violator and the number of violations. HIPAA's penalties are as follows.

a. If the violator did not know it was a violation--$100 up.
b. If there was reasonable cause for the violation--$1,000 up.
c. If there was willful neglect, but the violation was corrected--$10,000 up.
d. If there was willful neglect, and the violation was not corrected--$50,000 up.

Jail time is also scaled.

a. Unknowingly violating or with reasonable cause—up to 1 year.
b. Under false pretenses—up to 5 years.
c. For personal gain or malicious reasons—up to 10 years.

HIPAA's maximum penalty for a violation of the identical provision in the same calendar year is up to $1.5 million.

FERPA, however, only has one penalty—withholding of all federal funds for repeated violations after a warning.

Fines in Utah should be levied with the consideration of whether they include the cost of notifying parents, remediating the impact of the disclosure, and preventing re-occurrence of the disclosure in the future. A differentiation can be made between the unintended release of personally identifiable data by an employee during the course of their assigned duties and the intentional misuse of student data for unauthorized purposes or the negligent mishandling of student data by a contractor.

There is no standard process for responding to a release of a student's personally identifiable information. When a release of a student's PII occurs, there needs to be a process ready to follow to mitigate the negative impact, recall the data, and prevent any further exposure.

Recommendations:

These general principles that have emerged from initial discussions.

1. Penalties for employees and contractors should be differentiated.
    a. Penalties for employees should be consistent with those for violation of other State laws and SBOE policies.
    b. Penalties for contractors should be severe enough to deter violations. These should include monetary, sentencing, and barring from conducting business in Utah.

2. Training for employees and contractors should be provided by USOE on the FERPA and State rules and best practices to reduce the risk of unintended violations.

3. Penalties for repeat violations should be multiples of those for initial violations.

4. Monetary penalties are preferable.

5. Removing an educator's license may be appropriate for a severe violation.

6. Including in a penalty the costs for notifying parents and students, remediating the disclosure, and preventing a reoccurrence is appropriate.

7. There needs to be a standard process for responding to the unintended release of PII. This should be included in the USOE and LEAs' Data Governance Plans.

Question 7: What funding is needed at USOE to support LEAs and to protect the rights and privacy of students?

LEAs, charter schools, and the Utah School for the Deaf and Blind need support to learn and implement best practices. These entities and third-party contractors need audit oversight to ensure compliance with laws, regulations, and best practices. USOE needs resources to ensure that students' rights and privacy are being protected in accordance with USOE and LEA Data Governance Plans.

LEAs need a common source of support from which they will receive consistent answers and dependable training. USOE is the best practice provider for that support.

USOE needs a full-time CPO to meet the demands of the privacy and security issues described here.

USOE needs full-time positions to train and support the LEAs' teachers, aides, volunteers, administrators, and school board members. These positions would document and create guidance on best practices, create implementation plans for the LEAs, document current LEA practices that can be leveraged by others, and generally support the creation and maintenance of the Data Governance Plans. Those USOE FTEs need supplies, travel funds, and funds for substitutes to provide to the LEAs to conduct their training activities.

USOE needs a full-time position to audit the LEAs, charter schools, the Utah School for the Deaf and Blind, and third-party contractors for compliance with the requirements of FERPA, other regulations, and best practices. This position should provide content for the training delivered by the support positions.

Recommendations:

1. Chief Privacy Officer at USOE (1 FTE)
   a. $150,000 (annual) Compensation and benefits
   b. $25,000 (annual) Travel and expenses for participation in LEA visits, NCES meetings, and statewide activities
   c. $75,000 Expenses and contracted services for policy and content development for training and guidance for LEAs

2. Privacy Support Managers at USOE (3 FTEs)
   a. $325,000 (annual) Compensation and benefits
   b. $60,000 (annual) Travel and expenses for visiting LEAs and attending training meetings and conferences
   c. $100,000 (annual) To conduct training and produce materials on best practices, Data Governance Plans, implementation plans, etc.

3. Privacy Auditor at USOE (1 FTE)
   a. $125,000 (annual) Compensation and benefits
   b. $25,000 (annual) Travel and expenses for audit and compliance reviews
   c. $25,000 (annual) For guidance resources and development

4. Metadata Dictionary Development

    a. $450,000 ($60,000 annual) USOE metadata dictionary acquisition and loading for public disclosure, LEA support, and SBOE/Legislature reporting

    b. $125,000 ($25,000 annual) LEA metadata dictionary acquisition and loading for USOE reporting, public disclosure, and local data governance

5. Security Plan Development
    a. $250,000 ($20,000 annual) USOE security plan development
    b. $250,000 ($40,000 annual) LEA security plans development, and best practice training and support