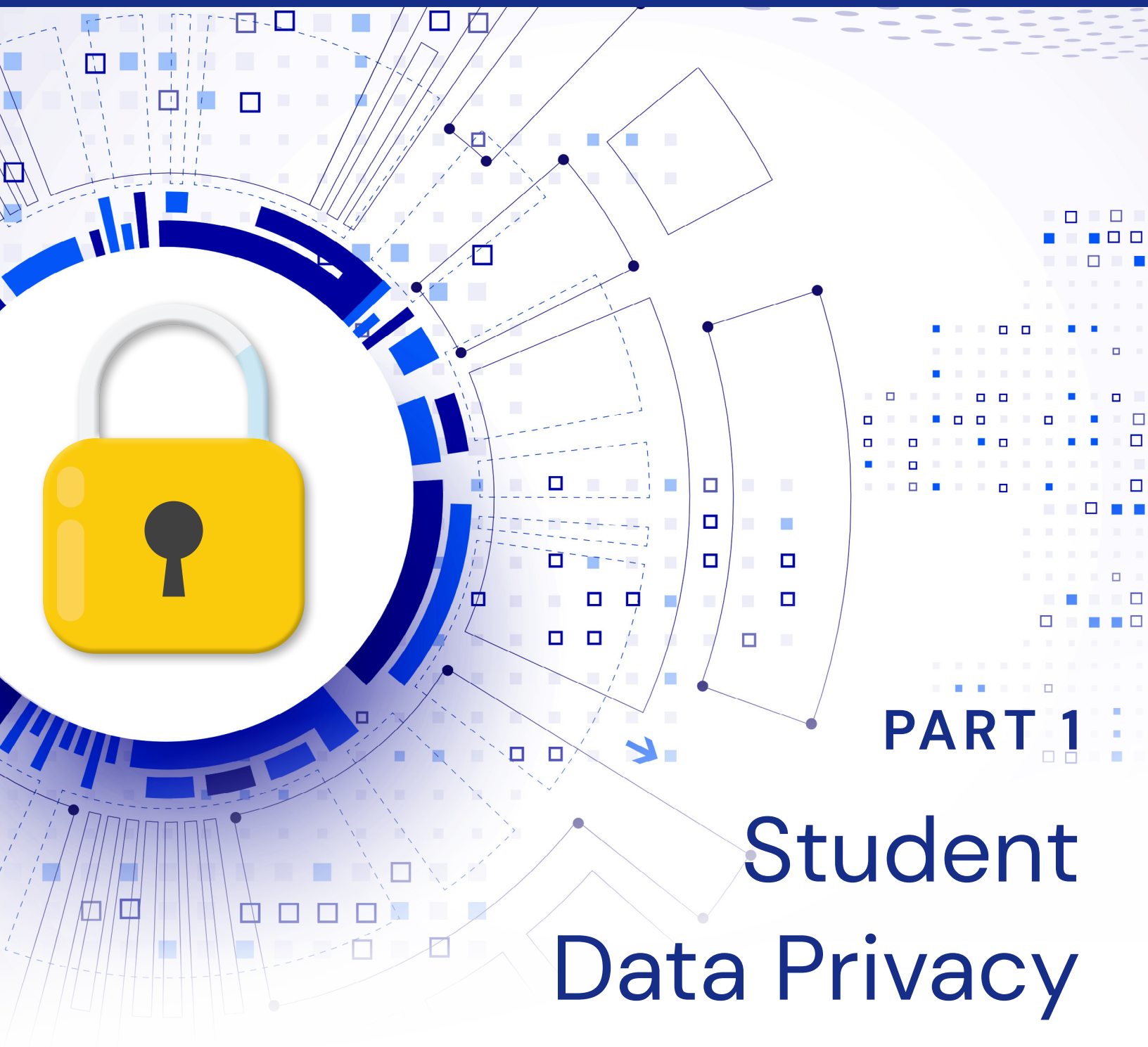
CoSN
LEADING EDUCATION INNOVATION

# CoSN Student Data Privacy Toolkit



PART 1

# Student Data Privacy Fundamentals

CoSN
LEADING EDUCATION INNOVATION

## About CoSN

The Consortium for School Network (CoSN) is the premier professional association for school system technology leaders. CoSN provides thought leadership resources, community, best practices and advocacy tools to help edtech leaders succeed in the digital transformation.

# Table of Contents

# Introduction

Protecting student data privacy is a foundational requirement for all School Systems. Successful engagement around the work requires development and ongoing maintenance of a holistic student data privacy program designed to guide and support all School System employees in maintaining focus on consistent implementation of robust policies and practices that are designed to address—at a minimum—the following 3 areas:

- **Ensuring compliance** with federal and state laws, board policies and contracts;
- **Preventing harm** to the student, or the School System (for example through a breach of sensitive personal information); and
- **Building trust** among parents and other community members, students, teachers, school board members, and legislators

This work requires that each School System develop and implement the measures appropriate to their ecosystem to help mitigate the risk while reaping the rewards of data-driven instructional programs to support student success.

Managing risk is not a new challenge in education. School Systems have a long history of continuously assessing risk and identifying and implementing an appropriate response, whether it be mandating use of goggles in the chemistry class, requiring safety gear and appropriate physical fitness for the football field, monitoring activity on the school bus, or assessing vendor technologies and implementing appropriate contractual controls around partner access to student personal information.

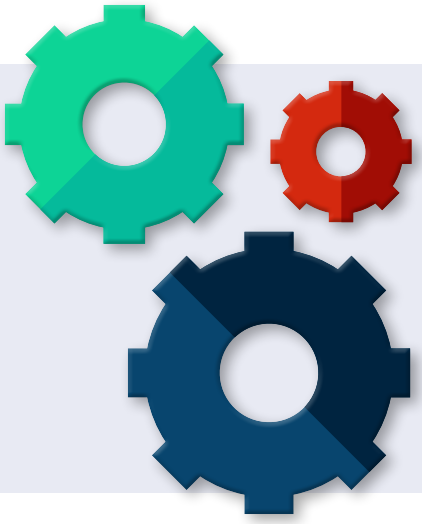
However, to accomplish any of this, School Systems leadership must be actively engaged. This is particularly important when it comes to building a student data privacy program, where true success depends on leadership investment to prioritize and champion the work across the organization.

Any student data privacy program must include concrete, documented policies, practices, and controls that provide adequate and appropriate protections around student personal information. Training of all school employees on their respective student data privacy obligations and security hygiene is also critical to the success of student data privacy and security programs, as are accountability measures.

To operate successfully, School Systems must also look beyond the basic privacy compliance practices and work to build trust within their local communities. By raising the bar on existing policies, practices, and controls, School Systems build the foundation from which they can build confidence in their communities. By engaging with parents about the School System's technology program and the scope of the existing student data privacy and security programs, School Systems ease concerns about student data privacy and earn the trust of community stakeholders.

It's no easy task. The policies and practices needed to comply with existing federal and state privacy regulations are numerous and complex, and the climate is continually shifting, with new state privacy laws refining existing requirements, while new technologies push the boundaries of what's possible. In addition, compliance with laws is generally considered to be the bare minimum standard of operational competence. To truly protect the privacy and security of student personal information, School Systems need to build a privacy program that permeates the organization, based on an understanding of what the laws require, how to implement those laws effectively across multiple technologies, and how to align with community expectations regarding data privacy and security in order to best leverage the power of information and technology to support student success.

This CoSN Student Data Privacy Toolkit is designed to help School Systems understand some of the fundamental requirements for protecting student data privacy. While much of the information presented here is specific to the protection of student personal information, it is hoped that the broader concepts might serve as important reminders for the protection of all personal information available to School Systems, informing larger frameworks for protection of personal information of employees and parents as well as students.



This CoSN Student Data Privacy Toolkit is designed to help School Systems understand some of the fundamental requirements for protecting student data privacy.

# Getting Started

What does a student data privacy management program look like, who needs to be involved, and what are the fundamental practices that School Systems should have in place to effectively manage data privacy and security responsibilities in a way that protects students, ensures compliance, and engenders trust in the community?

According to the US Department of Education's (ED) Privacy Technical Assistance Center (PTAC), an effective student privacy program improves the efficiency of district decision-making and operations regarding data collection, dissemination, and use of student data. In addition, a student privacy program:

- Helps districts meet legal and ethical requirements for protecting personally identifiable information in student Education Records;
- Protects students from harm (e.g., identity theft, discrimination, predatory activity); and protects the district from harm (e.g., loss of public confidence, administrative burden of investigating a breach, alienating parents, financial loss);
- Improves communication and transparency with parents and students about data practices, and helps to reassure parents and students about the privacy and security of their personal information.

Whether you're just getting started with your approach to protecting the privacy of students, or are looking to improve your practices, a fundamental part of the process should be establishing your own frameworks of behavior around management of student data. This includes understanding applicable laws and also understanding community norms and institutional goals, then combining that with the institution's mission to serve as the backbone of the program.

Without all of those factors brought in for consideration, a School System misses the opportunity to build a privacy program that is truly effective in operation. For example, relying only on an understanding of applicable laws can sometimes mean making decisions that are not wholly supported by parents, or are not in the best interests of your student community. After all, even if something is legally allowed, that does not mean that it will be the right fit for your School System. It can also mean missing out on the opportunity to apply consistent legal frameworks for situations not yet contemplated by laws.

Two useful starting points for frameworks are PTAC's Checklist for Developing School District Privacy Programs and the National Forum on Education Statistics Guide to Education Data Privacy.

## *Here are some key steps you'll need to manage:*

1. Engage with leadership to acknowledge the need and support for a privacy program, or to improve the existing program.
2. Designate an individual responsible for policies relating to student data privacy, including use of personal information.
3. Bring the right people to the table. Remember that everyone has a role to play in protecting student data privacy, so be sure that key stakeholders are engaged in developing a student data privacy program to build broader organizational understanding of the task at hand.
4. Determine which policies and procedures are already in place.
5. Adopt any additional necessary policies and procedures for the use of student data throughout the data life cycle, including consequences for non-compliance; update existing policies that may have fallen out-of-date.
6. Train those with access to student personal information on relevant policies and procedures to help them understand expectations for behavior.
7. Consider how best to be transparent with parents, students, and other community members about your privacy practices.
8. Develop a monitoring plan to ensure policies and procedures are being followed.

To begin the conversation with leadership, we encourage you to review the Student Data Principles. The Principles were created by a coalition of national stakeholders led by CoSN and Data Quality Campaign, who set out to determine a set of fundamental beliefs for using and protecting student data to guide the work of the education community.

## *Additional Resources:*

- Protecting Privacy: Making the Case to Leadership
- Student Data Privacy: A School System Priority. An Essential Commitment
- Trusted Learning Environment: The Role of Leadership in Protecting Student Data Privacy
- School System Privacy Stakeholders

# Toolkit Definitions

### *We use the following terminology across the Student Data Privacy Toolkit:*

- **School System:** an educational agency, including a school, district, or other local education agency.
- **Student Data:** any student information that is protected under applicable federal or state privacy law, including information that identifies, relates to, describes, could reasonably be associated with or could reasonably be linked, directly or indirectly, with an individual student. Student Data is also referred to as personally identifiable student data or student personal information.
- **Provider:** a technology company, community service provider, or other School System partner that has access to Student Data.
- **Privacy:** practices governing the collection, use, handling, disclosure, and deletion of Student Data, with a primary focus on the individual's personal right to be free from intrusion.
- **Security:** protections designed to preserve the confidentiality, integrity, and availability of Student Data and to prevent unauthorized access to and disclosure of Student Data.
    - **Privacy** and **security** are related disciplines, but they are not interchangeable. Both a privacy program and a security program are needed to properly protect Student Data.

# Legal Definitions

Federal student data privacy laws define similar terms in different ways, and it's important to understand the distinctions. Please also note that state laws include different definitions of similar terms. Be sure to familiarize yourself with the definitions presented here and compare them with definitions that may be included in your state's student data privacy legislation. By considering the entire ecosystem of legal definitions, you'll be better positioned to properly assess and grow your data privacy practices.

| Family Educational Rights and Privacy Act (FERPA) | Children's Online Privacy Protection Act (COPPA) |
|---|---|
| **Personally Identifiable Information (PII):**<br>Includes, but is not limited to:<br><br>The name of a student or family members; the address of a student or family members; a personal identifier, such as the student's social security number, student number, or biometric record; *other direct or indirect identifier 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 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.<br><br>  | **Personal Information (PI):**<br>Individually identifiable information collected from a child under the age of 13 online, including:<br><br>First and last name; address or other geolocation information that identifies a street name and city or town; email address or other online contact information that allows direct contact with a person online, including a screen or user name that functions in that same manner, telephone number, Social Security number; a persistent identifier that can be used to recognize a user over time and across different websites or online services; a photograph, video, or audio file that contains a child's image or voice, or information about the child or the child's parents or legal guardians that the operator collects online from the child and combines with one or more of the above identifiers. |

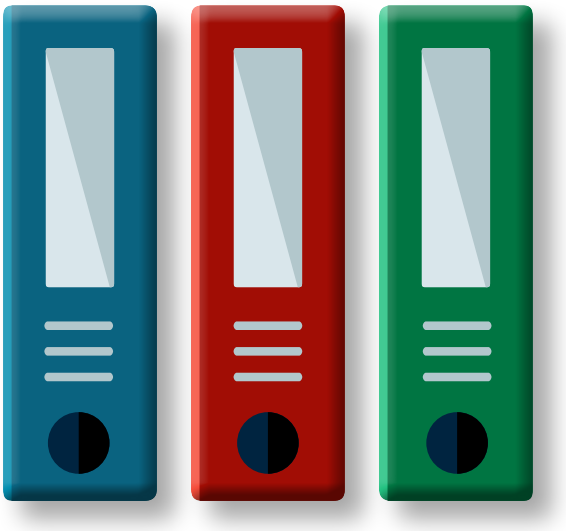
*Continues.*

| Family Educational Rights and Privacy Act (FERPA) | Children's Online Privacy Protection Act (COPPA) |
|---|---|
| **Education Records:**<br>Materials that are "maintained by an educational agency or institution or by a party acting for the agency or institution," and that contain information directly related to a student.<br><br>For more information about Education Records, including details of what is not considered an Education Record, see below. | |
| **Directory Information:**<br>Information in the Education Record that is not considered to be harmful or an invasion of privacy if released. **Each School System must define what it considers to be Directory Information.** Directory Information may include a student name, address, telephone number, email address, photograph, date/place of birth, major, grade level, enrollment status, date of attendance, degrees, honors/awards, most recent educational institution attended, participation in officially recognized sports and other activities, and weight and height of members of athletic teams.<br><br>Directory Information may not include a social security number. It may also not include a student ID that may be used to gain access to Education Records without additional information known to the individual.<br><br>For more information about Directory Information, see **FERPA: The Directory Information Exception**. | |
| **De-Identified Data:**<br>All personally identifiable information has been removed and *a reasonable determination has been made that a student is not personally identifiable, whether through single or multiple releases of information, and taking into account other reasonably available information*.<br><br>For more on De-Identified Data, and a discussion of aggregated data, see **Understanding Metadata and De-identification in CoSN's Student Data Privacy Toolkit Part 2: Working with Technology Providers**. | |

## *Education Records*

Just what is or is not an Education Record is not always clear-cut. A common misstep is often determining that because a Provider is not collecting log in credentials from students, there is no Student Data being collected and no Education Record being created. However, that is not always the case. Be sure to consider other factors, such as whether tracking technologies are used, student progress is saved, or if teachers might provide student roster information. Assess whether or not the records or information being collected, generated, stored or processed by a Provider qualify as an Education Record with your School System's legal counsel before proceeding. If they are, you will need to ensure that the handling of those records is done in alignment with FERPA requirements.

As noted in the Definitions section, Education Records are materials "maintained by an educational agency or institution or by a person acting for the agency or institution," and that contain information directly related to a student. However, the definition of "Education Records" is subject to certain exceptions. The following are **NOT** considered Education Records:



- Records kept by the person who made them that are used only as a "personal memory aid" and not disclosed to anyone, except a temporary substitute
- Records maintained by an educational agency's law enforcement unit
- Employee records made in the normal course of business that pertain only to the individual's employment and that are not used for any other purpose
- Records created about a student age 18 or older or who is attending a postsecondary education institution by professionals such as a physician, psychiatrist, psychologist or other recognized professional or paraprofessional acting or assisting in that capacity for treatment of the student; this information can only be disclosed to those who provide the treatment
- Records that an educational agency created or received after the student stopped attending the institution and that are not directly related to the individual's attendance as a student
- Grades on peer-reviewed papers before they are collected and recorded by a teacher

For more information, see the US Department of Education's (ED's) Protecting Student Privacy While Using Online Education Services: Requirements and Best Practices and National Center for Education Statistics Forum Guide to the Privacy of Student Information.

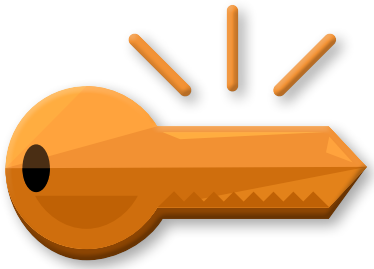
# The Family Educational Rights and Privacy Act (FERPA): Select Requirements

The following illustrates some of the core requirements in FERPA and attempts to support School Systems in better understanding some challenging areas of the law. There is, of course, much more to FERPA than what is explained here, and as with all the laws discussed in this Toolkit, we hope this will help to inform larger discussions with your legal counsel.

## *Education Records: Rights of Parents and Eligible Students:*

A key concern of FERPA is ensuring that parents and eligible students—those students who are 18 years of age or older, or are attending a postsecondary education institution—may:

- Inspect and review the student's education records;
- Seek amendment of the student's education records that the parent or eligible student believes to be inaccurate, misleading, or otherwise in violation of the student's privacy rights;
- Consent to disclosures of personally identifiable information contained in the student's education records, except to the extent that FERPA authorizes disclosure without consent; and
- File a complaint with ED concerning alleged failures by the School System to comply with FERPA requirements.



School Systems are required to advise parents and eligible students of these rights in an annual notice. This notice must be provided via any means that are "reasonably likely" to inform parents and eligible students of their rights, and School Systems must be sure to effectively notify those individuals who are disabled and parents of K12 students who have a primary home language other than English.

School Systems must respond to requests to inspect and review the student's Education Records in a "reasonable period of time frame," upon receipt of the request, not to exceed 45 days. Some state laws impose shorter time frames, so School Systems should be familiar with their state requirements, and have policies and processes in place to respond to these requests in a timely and comprehensive manner. Such policies and processes should include obtaining access to information in the Education Record that may have been disclosed to a Provider, as described below.

### Moving From Compliance to Trust

*Maintaining the accuracy and integrity of Student Data should be part of any School System compliance program. In fact, accuracy and integrity are fundamentals for any data privacy program. Making decisions based on inaccurate or incomplete student records can cause harm to the student, so keeping records current and complete is critical to protecting student privacy and leveraging the information to make effective decisions that benefit students.*

## *Disclosing Student Data: Select FERPA Obligations*

Before disclosing Student Data, FERPA requires that School Systems first obtain written consent from the parent or eligible student. However, there are a number of exceptions to that requirement in FERPA, all of which are designed to support School Systems in their typical and expected operation as education institutions, while maintaining appropriate protections over Student Data.

This Toolkit explores some of the commonly used exceptions. When considering these exceptions, it can be helpful to think of them as operating independently of one another. For example, as noted below, a parent or eligible student may choose to opt out of having their information categorized as Directory Information. If that happens, that does not mean that the Student Data couldn't still be disclosed under the School Officials exception. Each exception operates under its own specific set of circumstances, with its own specific requirements.

### FERPA: The School Officials Exception

One of the most common ways in which you may disclose personally identifiable information from Education Records to both your employees and Providers is by designating that party as a School Official. However, in order to do that, the person or entity with which you are disclosing information must meet certain criteria.

To decide whether or not the criteria have been met, you must be able to answer "yes" to the following:

- ☐ Is the person a teacher or other employee within your educational agency, with a legitimate educational interest in the records you would like to disclose?
  - ☐ Each School System must define what it considers to be a legitimate educational interest, and must disclose this definition to parents in the legally required annual notice, along with information about how it qualifies an individual or entity as a School Official. The School System must also determine whether or not the person whom you might qualify to be a School Official has a legitimate educational interest to access and use the Student Data in a manner that is **consistent with your established definition of legitimate educational interest,** as well as with any School System policies on this matter.

- ☐ You must use what ED refers to as "reasonable methods" to ensure that all of your School Officials are provided with access to only the personally identifiable information in Education Records in which they have a legitimate educational interest. When working with your employees (and Providers), consider what information they *need to know,* compared with what information might be convenient for them to have. "Need to know" should be the standard through which you operate.

***OR***

☐ Is the person or entity a contractor, consultant, volunteer or other party to whom you have outsourced institutional services or functions?

- ☐ If so, does the contractor, consultant, volunteer or other party meet **ALL** of the following criteria:

  1. They perform an institutional service or function for which you would otherwise use employees
  2. They are under your *direct control* with respect to the use and maintenance of Education Records;
     - In determining whether or not you have "direct control" of how the Provider may use and maintain the Education Records, consider whether or not you have a contract with the Provider that details—in the words of ED—"all of the necessary legal provisions governing access, use and protection of the data." For more on contract fundamentals, see **Contracts and Terms of Service in CoSN's Student Data Privacy Toolkit Part 2: Working with Technology Providers**.
  3. They are bound to use the personally identifiable information in the Education Records only for the purpose for which you disclosed it, and for no other purpose unless they first obtain the written consent of the parent or eligible student.*

** Please keep in mind that your state laws may have additional requirements around redisclosure of personally identifiable information, and you should become familiar with those restrictions to be sure you understand the extent of the legislative landscape and articulate those restrictions in contracts with your Providers.*

When working with Providers, they too, must only receive access to the minimally required personally identifiable information in Education Records in which they have a legitimate educational interest. In order to assess that, you'll want to review the Provider's Privacy Policy, which should explain what Student Data they collect, and how they use and share it.

Remember that as a School System, you are not authorized to allow a Provider to use personally identifiable information from Education Records for commercial purposes, only for purposes that serve the legitimate educational interest. As noted above, you also need a contract with the Provider that establishes your "direct control" over how the Student Data is to be managed, including agreement on what Student Data will be disclosed, what it may be used for, how it must be secured and how and when it must be securely destroyed.

In all cases, you must use physical, technological and/or administrative controls to ensure that Student Data is disclosed only to those who have a legitimate educational interest in receiving it.

### Example of School Official and Permitted Uses of Data

"A district contracts with a Provider to manage its cafeteria account services. Using the ***School Official exception,*** the district gives the Provider student names and other information from School System records …. The Provider sets up an online system that allows the School System, parents, and students to access cafeteria information to verify account balances and review the students' meal selections. The Provider cannot sell the student roster to a third party, nor can it use PII (personally identifiable information) from Education Records to target students for advertisements for foods that they often purchase at school under FERPA, because the Provider would be using FERPA-protected information for different purposes than those for which the information was shared."—*PTAC*

**More Information:** ED's *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices* and *Future of Privacy Forum's, Who Is a School Official Anyway?*

## FERPA: The Directory Information Exception

As noted below, a School System may disclose Directory Information without obtaining prior written consent from the parent or eligible student, as long as the School System notifies the parents or eligible students of the Student Data to be disclosed, and provides the parent or eligible student with a means to opt out of that disclosure and a reasonable amount of time to do so.

Classifying certain data elements as Directory Information allows School Systems to conduct some fundamental and often expected practices, such as publishing team rosters, the program for the school play, or the student yearbook, without first obtaining prior written consent from the parent or eligible student.

The Definitions section lists the types of information that a School System may choose to designate as "Directory Information."

As noted by ED, each School System must:

1. Define what it considers to be Directory Information, consistent with the requirements and limitations on that information as set forth in FERPA;
2. Provide public notice of the types of information which they have designated as Directory Information,
3. Give parents or eligible students the right to opt out of having their personal information classified as Directory Information, effectively opting them out of disclosure of that information under the Directory Information exception.
    - Notification to parents and eligible students about their rights over Directory Information must include the period of time during which they have to provide written notice in order to opt out of having the School System designate the Student Data as Directory Information.

### Limited Release Policy for Directory Information:

Objections to release of Directory Information frequently occur when parents are unclear about who might receive the information, or whether or not it would be disclosed for commercial purposes unrelated to the School System.

One option for a more privacy-friendly approach to Directory Information is to implement a limited Directory Information release policy. Under this type of policy, a School System may either (a) designate the specific entities that may receive Directory Information, or (b) designate the specific purposes for which Directory Information may be disclosed.

> *"In its public notice to parents and eligible students in attendance at the agency or institution…an educational agency or institution may specify that disclosure of directory information will be limited to specific parties, for specific purposes, or both."*[1]

Remember that in adopting a limited release policy for Directory Information, the School System MUST abide by the limitations that it describes in the required annual notice. If a School System wants to disclose Directory Information for a purpose not specified in the notice, it must provide parents and eligible students with an additional notice and the opportunity to opt-out of such disclosure.

See National Center for Education Statistics Forum Guide to the Privacy of Student Information for more information.

[1] https://www.ecfr.gov/current/title-34/subtitle-A/part-99

## Frequently Asked Questions about Directory Information

1. **Can a School System use the Directory Information exception to create student accounts in a Provider product if that is the only information required?**
   The Directory Information exception was not intended to be used to share Student Data with Providers.

   ED points out that disclosing Student Data with a Provider under this exception has two major drawbacks:

   - First, only Directory Information specified in the public notice may be disclosed using this exception. Remember that the Provider may be collecting data elements that are not considered Directory Information (but that may be Student Data) through the use of tracking technologies.
   - Second, the fact that parents and eligible students may, and often do, "opt out" of disclosing their Directory Information can create an imbalance in the classroom environment or in administrative systems if some students have been opted out of disclosure while others have not.

   Additional risk may be created if the student will create data through the use of a Provider's product or service that should be treated as part of the Education Record. In addition, if the School System relies on the Directory Information exception to share Student Data with the Provider, instead of relying on the School Officials exception, the School System is not likely to have the necessary direct control over that Student Data. This can leave the School System with no effective means to control the Provider's use and maintenance of the Student Data.

   Lastly, if the Provider collects data from the student and uses that data for marketing purposes, the Protection of Pupil Rights Amendment (PPRA) may apply, and again, the School System will not be in a position to meet its legal requirements if it has shared the Student Data with the provider by leveraging the Directory Information exception instead of the School Official exception.

   Therefore, ED suggests that the School Officials exception is likely a better option for School Systems when disclosing Student Data to a Provider.

2. **What special precautions do School Systems need to take regarding categorizing Student IDs as Directory Information?** The 2008 amendments to FERPA allow the categorization of the Student ID as Directory Information when the Student ID is an identifier for electronic systems, AND when the identifier is **combined with other authentication factors known only to the user,** such as a password. The idea here is that the Student ID may be categorized as Directory Information only when the Student ID is not, in and of itself, identifiable of the student, and is not attached to other identifiable information.

Per ED, "This will prevent districts and institutions from attaching these identifiers to students' names on sign-in sheets in classrooms, health clinics, etc.; prevent schools from disclosing lists with these identifiers attached to students' names, addresses, and other Directory Information; and prevent teachers from using them to post grades.

This is intended to help reduce the risk of unauthorized access to personal information and identity theft by ensuring that schools do not make these identifiers available publicly.

School Officials will still be able to use class lists with ID numbers but cannot make them available to students or parents. Teachers that still post grades publicly will have to use a code known only to the teacher and the student."

This means that Student ID cannot be considered Directory Information when posting grades or other student work, or as the sole means of access to student information or services (e.g., logging in to a website, checking out library books, or paying for lunches).

In order to consider the Student ID as Directory Information, the school must:

- Declare this use in their notice AND
- Ensure that it is combined with some other identifier known only to the user.

(As noted above, parents and eligible students may opt out of Directory Information disclosures. When that happens, if the Student ID has been designated as Directory Information, those students will not be able to participate in Provider services that require a Student ID if the information is disclosed to the Provider under the Directory Information exception of FERPA. See FERPA Final Rule 34 CFR Part 99 Section-by-Section Analysis December 2008.)

## *FERPA: Research and Studies Exceptions*

Two other commonly used, and sometimes confused, exceptions to the requirement that School Systems obtain written consent from the parent or eligible student prior to releasing Student Data from the Education Record are the Research and the Studies exception.

### FERPA Research Exception

The FERPA Research exception is typically used when a School System is conducting or is engaging with a Provider to conduct education research, including longitudinal research.

Under this exception, the School System or may release **de-identified** student level data from Education Records in order to conduct education research by attaching a code to each record that may allow the recipient to match information received from the same source over time, provided that—

(i) The party that releases the de-identified data does not disclose any information about how it generates and assigns a record code, or that would allow a recipient to identify a student based on a record code;

(ii) The record code is used for no purpose other than identifying a de-identified record for purposes of the education research and cannot be used to ascertain personally identifiable information about a student; and

(iii) The record code is not based on a student's social security number or other personal information.

### FERPA Studies Exception

FERPA permits School Systems and state education agencies (SEAs) to release Student Data to a Provider without first obtaining prior, written consent from the parent or eligible student when the Provider is under contract to conduct studies for or on behalf of the School System in order to:

- Develop, validate, or administer predictive tests;
- Administer student aid programs; or
- Improve instruction.

In order to leverage this exception to the consent requirement, the School System or SEA must ensure that:

(i) The study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information;

(ii) The Student Data is destroyed when no longer needed for the purposes for which the study was conducted.

School Systems and SEAs wishing to partner with third parties to conduct studies must do so under a written agreement with the Provider. That agreement must:

(i) Specify the purpose, scope, and duration of the study or studies and the information to be disclosed;

(ii) Require the Provider to use personally identifiable information from education records only to meet the purpose or purposes of the study as stated in the written agreement;

(iii) Require the Provider to conduct the study in a manner that does not permit personal identification of parents and student by anyone other than representatives of the organization with legitimate interests; and

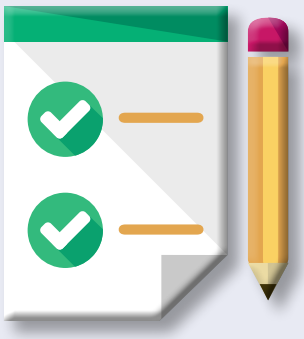
(iv) Require the Provider to destroy all personally identifiable information when the information is no longer needed for the purposes for which the study was conducted and specifies the time period in which the information must be destroyed.

# The Protection of Pupil Rights Amendment (PPRA) At-a-Glance

PPRA applies, with some minor exceptions, to sensitive data collected directly from the student via any program that receives funding from ED. Generally, the PPRA requires School Systems to obtain prior written consent from parents or students over the age of 18 or emancipated minors before administering a survey, analysis or evaluation that requires students to disclose any of the following sensitive information:

- Political affiliations or beliefs of the student or the student's parent
- Mental and psychological problems of the student or the student's family
- Sex behaviors or attitudes
- Illegal, anti-social, self-incriminating, or demeaning behavior
- Critical appraisals of individuals that have a close family relationship with the student
- Legally privileged or analogous relationships, such as conversations with doctors, lawyers or clergy
- Religious practices, affiliations, or beliefs of the student or the student's parent
- Income (other than information required by law to determine eligibility for financial aid)

### The PPRA in the Modern Classroom Environment



When considering the application of the PPRA to your School System activities, be sure to include consideration for questions that may come up in social-emotional learning curricula, as well as early intervention programs designed to help identify and support students who may be at risk.

These types of programs often implicate the PPRA requirements, so thoughtful program design and consideration for the rights of students—including the most vulnerable student populations—and your obligation of care to your students—will help you avoid potential privacy harms.

If funds from ED are not used for such surveys, but such surveys are conducted with information collected directly from the students, School Systems must still notify parents, at least once at the beginning of the school year, of:

- The date(s) when the surveys may be conducted;
- The right to opt their child out of participating; and
- The right to request for review any instructional materials used in connection with any survey that involves the subject matter noted above and those used as part of the educational curriculum.

These requirements apply regardless of whether or not the School System administers the survey directly or uses a Provider to administer it. However, if a Provider administers the survey on behalf of the School System, contractual clauses should be in place restricting the Provider's use of the information obtained from students only to serve the school purpose.

### *PPRA Policy Development*

Under the PPRA, School Systems are also required to consult with parents in relation to developing and adopting policies addressing:

- That parents have the right to inspect, upon request, a survey created by a third party before the survey is administered or distributed by a school to students, and the procedure for granting a request by a parent for such access;
- How the School System will protect the privacy of student information in the event that a survey is administered to students that contains subject matter described above, and the right of parents to inspect, upon request, a survey that concerns one or more of the eight protected items of information;
- The right of parents to inspect, upon request, any instructional material used as part of the educational curriculum for students, and the procedure for granting a request by a parent for such access;
- Administration of physical exams or screenings of students;
- The collection, disclosure, or use of personal information (including items such as a student's or parent's first and last name, address, telephone number or social security number) collected from students for marketing purposes, or to sell or otherwise provide the information to others for marketing purposes, including the School System's arrangements for protecting student privacy in the event of collection, disclosure, or use of information for these purposes; and
- The right of parents to inspect, upon request, any instrument used in the collection of personal information for marketing or sales purposes before the instrument is administered or distributed to a student and the LEA's procedure for granting a parent's request for such access.

The PPRA does allow School Systems to collect, disclose or use personal information collected from students to develop, evaluate or provide educational products or services for the students or the School System without creating a policy for such practices. Generally, this includes activities such as:

- College or other postsecondary education or military recruitment
- Book clubs, magazines, and programs providing access to low-cost literary products
- Curriculum and instructional materials used by elementary schools and secondary schools
- Tests and assessments used by elementary schools and secondary schools to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students (or to generate other statistically useful data for the purpose of securing such tests and assessments) and the subsequent analysis and public release of the aggregate data from such tests and assessments
- The sale by students of products or services to raise funds for school-related or education-related activities
- Student recognition programs

Keep in mind that these information use rights need to be assessed in conjunction with FERPA and COPPA requirements, as well as state law restrictions. In short, **just because something is permissible under PPRA or another law, does not mean that a School System may actually engage in that activity.** The full matrix of legislation needs to be considered as a whole, for each use case.

### Parental Notification and Opt-Out

If a School System participates in any of the following activities, it must notify parents and students age 18 and older as follows:

| Activity | Minimally Required Notice |
|---|---|
| Where lawful, with consideration for not just the PPRA but also state laws, the collection of Student Data directly from students to use for marketing or to sell to another party. | Notify parents and students 18 and older of policies surrounding these activities; be mindful of additional or conflicting state law limitations and community norms with respect to this activity. |
| Any survey that asks students to provide sensitive information as defined in the PPRA. | Request permission from parents prior to providing such surveys to students. |
| Any invasive, non-emergency physical examination or screening that is required as a condition of a student's school attendance, administered by the school and scheduled by the school in advance, not necessary to protect the immediate health and safety of the student or of other students, and not required or permitted by state law. | Notify parents and students 18 and older of times and dates when you plan to perform any of these activities. |

Note also, that parents have certain opt-out rights under PPRA, which must also be implemented. For more information on the PPRA as it applies to online contexts, see What is the Protection of Pupil Rights Amendment? and Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices.

# State Student Data Privacy Laws: A Brief Overview

No discussion of student data privacy would be complete without consideration for US state student data privacy laws. Most states have their own student data privacy law, or a combination of laws, focused on:

- Student data privacy governance requirements and prohibitions for School Systems;
- Requirements for School Systems when working with Providers;
- Student data privacy governance requirements and prohibitions for Providers;
- Student data security requirements;
- Record-keeping and transparency requirements;
- Parent rights.

The specifics of each law vary, as do the enforcement mechanism. However, there are some common themes across the requirements, including:

- Expanded definitions of the student information to be protected;
- Reiteration and expansion of, and updates to certain requirements first articulated in FERPA, including concepts related to:
  - Limitations on use of Student Data for the educational purposes (often referred to as the "K-12 purpose");
  - Parent rights;
  - School System's direct control over the use and maintenance of Student Data

State laws also typically emphasize the following:

- Limitations on use and disclosure of Student Data, supporting core privacy tenants of data minimization and access limitations;
- Data deletion requirements, often triggered when the Student Data is no longer needed for the purpose for which it was provided (reflecting another core privacy tenant), or otherwise when the contract with the Provider terminates or within a reasonable time period after termination;
- Strict prohibitions on use of Student Data for targeted advertising;
- Implementation of what the Federal Trade Commission would consider to be "reasonable security."

Of course, each state student data privacy law is unique, and this is not intended to be a primer on your applicable state student data privacy laws. However, it is important to understand that the state student data privacy laws are additive to the federal laws, not a replacement. Review your state student data privacy laws carefully and consult with your counsel for support on building the necessary components to your student data privacy program to ensure you are operating consistently with both federal and state requirements.

# The Children's Online Privacy Protection Act (COPPA) in Context

Although FERPA leads the way as the key federal law regulating how School Systems manage student data privacy, and the PPRA regulates collection of information from students about sensitive subjects and use of Student data for marketing purposes, it can be helpful to take a closer look at an equally important federal law that regulates how Providers must protect the privacy of personal information collected directly from children under the age of 13.

## *First, which law applies where?*

| FERPA | PPRA | COPPA |
|---|---|---|
| Applies to School Systems that receive funding from ED.<br><br>The Provider should align with applicable provisions of FERPA and work with the School System to support the School Systems' use of the Provider's product or service in compliance with FERPA. | Applies to School Systems that receive funding from ED.<br><br>The Provider should align with the applicable provisions of PPRA and work with the School System to support the School Systems' use of the Provider's product or service in compliance with PPRA. | Applies to operators of commercial websites and online services that are directed to children under 13 and that collect, use, or disclose personal information from children under 13, or that have actual knowledge that they are collecting personal information from children under 13, either directly or from users of another website or online service directed to children under 13.<br><br>The Provider may rely on a contract with a School System, including a click-wrap agreement, to indicate that the School System has obtained the necessary parental consents to collect the data. However, the Provider must supply the School System with advance notice of its information collection, use and disclosure practices, so that the School System may make an informed decision. (See FTC's Complying With COPPA Frequently Asked Questions.) |

The truth is that at any given time, any or all of the laws may apply. While the flowchart below takes you through a decision tree about FERPA, COPPA and PPRA, it's equally important to understand that the laws are not mutually exclusive.

## *What Data Is Protected?*

| FERPA | PPRA | COPPA |
|---|---|---|
| Education Records, including personal data collected from and about parents and students. | Personal data collected by a School System or Provider from students about specific, sensitive subjects or to develop, evaluate or provide educational products or services as described above. | Personal information collected from children under the age of 13. |

Regardless of the law, parents retain certain rights around the collection, use and sharing of their child's data. Some of these are listed here:

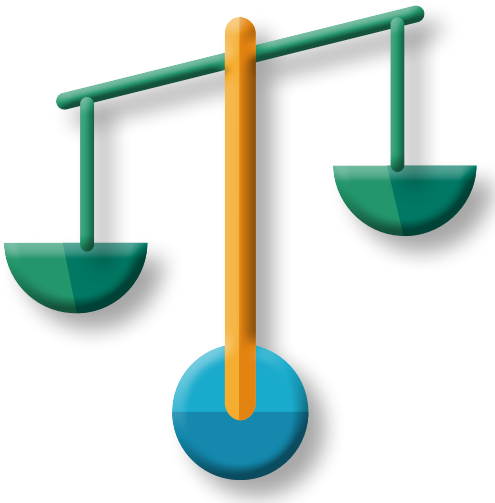
| FERPA | PPRA | COPPA |
|---|---|---|
| Right to review the student's Education Record and request amendment of errors.<br><br>Must consent to sharing of their child's personal information, unless that information is sent to a Provider or other party operating as a designated School Official or under another applicable exception.<br><br>Right to opt out of sharing what a School System has designated as Directory Information. | Right to review surveys or similar materials requesting information from students about specific, sensitive subjects and opt their child out of participating.<br><br>Must be part of policy development related to access to the materials referenced above, instructional material related to the curriculum, administration of physical exams and marketing prohibitions, with certain limited exceptions. | Must provide prior, verifiable consent for collection, use and disclosure of their child's personal information except in limited circumstances.<br><br>Right to review information collected from their child, request that it be deleted and/or request that no additional personal information be collected from their child. |

When working with Providers, **be sure you consider all of these laws,** including your state student data privacy laws, which may include additional requirements and restrictions.

# Navigating Key Federal Laws: Getting Started

### Some questions to consider:

- Who is collecting the information? Is it the School System or the Provider?
  - If it is collected by the School System, consider FERPA and PPRA.
  - If it is collected by the Provider, consider FERPA, PPRA and COPPA
- Is the information being collected directly from the student?
  - If so, consider FERPA and PPRA
    - Is the student under age 13?
- If so, consider FERPA, PPRA, and COPPA
- Is parental consent needed to disclose the Student Data to a Provider?
  - Who is obtaining the consent, the School System or the Provider?
    - Remember that under COPPA, the Provider may rely on the School System to obtain parental consent on its behalf only when the student's personal information will be used for the school purposes and not for any commercial purpose.

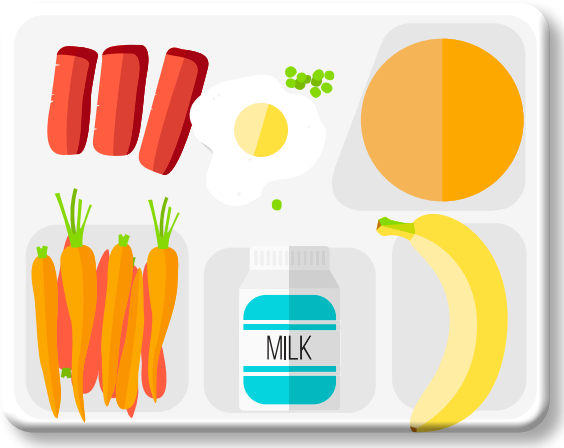


- Will the Student Data be used for marketing purposes authorized by your School System?
  - Is the use consistent with your School System policy?
  - Have you managed compliance with PPRA?
  - Has the Provider obtained consents directly from parents in compliance with COPPA if personal information is to be collected from students under 13, considering that the School System may not authorize a commercial use?
  - Have you consulted your state law, which may prohibit this activity?

It is an undeniably complex ecosystem, but considering these questions as you assess where and with whom you disclose Student Data will help ensure that you are properly managing your responsibilities across all legislative requirements.

# National Student Lunch Act (NSLA) At-A-Glance

Although not specifically a student data privacy law, the National Student Lunch Act ("NSLA") does contain privacy requirements that are worth noting. The Act established the National Student Lunch Program, which provides free and low-cost lunches to students. At the federal level, the program is administered by the Food and Nutrition Service, and at the state level, it is usually administered by state education agencies through agreements with School System food authorities.




The Program is open to all School Systems—public, nonprofit, private, independent—and as such, the Act requirements apply to all as well.

From a privacy perspective, the Act limits use or disclosure of information obtained from an application for a free or reduced price meal. Such information is only available to:

- A person directly connected with administration or enforcement of the Act,
- A federal education program,
- A state health or education program administered by the State or local educational agency, or
- Certain qualified federal, state or local nutrition programs, the US Comptroller General and local law enforcement investigating compliance.

Even then, the information provided must be limited to income eligibility unless consent is obtained from the student's parent or guardian.

Those who do receive the information are prohibited from disclosing it.

In short, within your School System, knowledge about who is eligible for free and reduced meals must be strictly limited, and care should be taken to ensure that these students are not identified—either directly or indirectly—as participants in the program.

For more information, see 42 USC 1751 and National Center for Education Statistics Forum Guide to Protecting the Privacy of Student Information: Other Federal Laws Affecting Information Privacy in Schools.

# Health Insurance Portability & Accountability Act (HIPAA) At-a-Glance

The Health Insurance Portability and Accountability Act ("HIPAA") was enacted in 1996 in an effort to set national standards for the transmission of sensitive health information. HIPAA mandates administrative, technical, and physical safeguards to ensure that individual health information remains private and secure. In 2009 the Health Information Technology for Economic and Clinical Health Act (HITECH[2]), part of the American Recovery and Reinvestment Act, incorporated new provisions into HIPAA's Privacy[3] and Security[4] Rules. HITECH established that the Department of Health and Human Services (HHS) would issue guidance regarding technological methods for protecting health information and extended HIPAA enforcement to service Providers or "business associates" who help manage and transmit health information on behalf of a "covered entity."

**While HIPAA is important to understand, its application in K12 schools is limited. Most student records, including health records, are Education Records, which are covered by FERPA.**

As noted in the U.S. Department of Health and Human Services and the U.S. Department of Education's *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records* (2008) ("Joint Guidance"), "At the elementary or secondary level, a student's health records, including immunization record…as well as records maintained by a school nurse, are Education Records subject to FERPA."[5] This is because these records are often directly related to the student and are maintained by the school for its purposes, rather than to process the transactions as noted above.

---

[2] You can access more information on the HITECH Act at http://www.hhs.gov/ocr/privacy/hipaa/ administrative/enforcementrule/hitechenforcementifr.html

[3] You can access more information on the HIPAA Privacy Rule at http://www.hhs.gov/ocr/privacy/hipaa/ understanding/summary/index.html

[4] You can access more information on the HIPAA Security Rule at http://www.hhs.gov/ocr/privacy/hipaa/ understanding/srsummary.html

[5] For more information, see the Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records (2008)

However, HIPAA likely applies to health information related to your School System employees, as well as to the transmission of health information for any of the following purposes:

- Process healthcare claims or equivalent encounter information
- Process health care payments and provide remittance advice
- Coordinate benefits
- Check or process health care claim status
- Enroll or process the disenrollment of individuals in a health plan
- Determine eligibility for a health plan
- Process health plan premium payments
- Certify and authorize referrals
- Process the first report of injury
- Manage and process health claims attachments
- Process health care electronic funds transfers (EFT) and remittance advice

If you are using an online service Provider to transmit your students' protected health information for any of the purposes set forth above, and that information is not part of an education record (as defined by FERPA) then you and your online service Provider need to comply with the obligations and security standards set forth in HIPAA and HITECH. In addition to the contractual provisions covered in the Contracts and Terms of Service section in Part 2 of this Toolkit, you should include an obligation to comply with HIPAA, and also have your online service Provider execute a *Business Associate Agreement*[6].

In any event, treating the health information of your students in accordance with the security standards and requirements dictated in HIPAA is generally a good practice, and can be a useful guide to securing your students' information more broadly.

[6] For a sample Business Associates Agreement, visit: http://www.hhs.gov/ocr/privacy/hipaa/understanding/ coveredentities/contractprov.html

# Next Steps

The CoSN Student Data Privacy Toolkit consists of 3 sections, each designed to provide you with information to help support your work in protecting student data privacy:

- Part 1: Student Data Privacy Fundamentals
- Part 2: Partnering with Service Providers
- Part 3: Transparency and Trust

We encourage you to download all 3 as part of your student data privacy resource library.

### Additional resources are available at CoSN.org/Privacy and below:

- The US Department of Education: FERPA Overview
- The US Department of Education Privacy Technical Assistance Center (PTAC)
- Complying with COPPA: Frequently Asked Questions, FTC
- An Overview of the Children's Online Privacy Protection Act and the Family Educational Rights and Privacy Act, Harvard Law School's Cyberlaw Clinic


## Acknowledgements:

CoSN would like to thank the CoSN Student Data Privacy Educator Advisory Panel for their work in creating this Toolkit. CoSN would also like to thank previous committee members, as well as Jim Siegl, Reg Leichty, Founder and Partner of Foresight Law + Policy, The Cyberlaw Clinic at Harvard Law School, Berkman Klein Center for Internet & Society at Harvard University, National School Boards Association Council of School Attorneys, and past and present sponsors of the CoSN Student Data Privacy Initiative for their work in creating the initial Toolkit and subsequent updates.