Confidentiality Law in Education

There are three federal laws and one Constitutional amendment that require understanding when addressing student privacy.
- The main law, FERPA, or the Family Educational Rights and Privacy Act.
- HIPAA or the Health Insurance Portability and Accountability Act.
- IDEA or the Individuals with Disabilities Education Act.
and PPRA, the Protection of Pupils Rights Amendment.

FERPA, the Family Educational Rights and Privacy Act affords parents
- the right to have access to their children's education records,
- the right to seek to have the records amended, and
- the right to consent to the disclosure of personally identifiable information from education records, except as provided by law.
– When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student, and he or she is known as an "eligible student" under FERPA.

As educators with privacy protection responsibilities, it's important to understand four key definitions:
Education Records, Personally Identifiable Information, Directory Information, and Disclosure

"Education Records" - those records that are directly related to a student and maintained by an educational agency or institution or by a party acting for agency or institution.

"Personally Identifiable Information" (PII) including, but not limited to
• the student's name;
• name of the student's parent or other family members;
• address of the student or student's family;
• a personal identifier, such as a social security number or student number
• other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name.
• other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
• information requested by a person who the educational institution reasonably believes knows the identity of the student to whom the education record relates.

"Directory Information" is "personally identifiable information" that is not generally considered harmful or an invasion of privacy if disclosed – including, but not limited to:
• name, address, telephone listing, electronic mail address;
• date and place of birth;
• photographs;

• participation in officially recognized activities and sports;
• field of study;
• weight and height of athletes;
• enrollment status (full-, part-time, undergraduate, graduate);
• degrees & awards received;
• dates of attendance;
• most recent previous school attended; and
• grade level.

"Directory Information" cannot generally include a student's social security number or student ID number.
"Directory Information" may include a student ID number or other unique personal identifier that is displayed on a student ID badge, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a PIN, password, or other factor known or possessed only by the authorized user.

Under FERPA, "Disclosure" means to permit access to or release, transfer, or other communication of personally identifiable information contained in education records by any means including oral, written, or electronic means, to any party except the party identified or the party that provided or created the record.

There are three types of disclosure—authorized, unauthorized, and inadvertent.

FERPA authorizes or permits specific users and uses of personally identifiable information in student education records without the written consent of the parent or eligible student. These authorized disclosures include, but are not limited to:
• other school officials, including teachers within the agency or institution who have legitimate educational interests;
• officials of another school or postsecondary institution in which the student seeks to enroll;
• authorized representatives of the Comptroller General of the United States, Attorney General of the United States, the Secretary of the U.S. Department of Education, and state and local educational authorities;
• in connection with financial aid for which a student has applied or received;
• State and local officials or authorities to whom access is granted under state statute;
• to comply with a judicial order or lawfully issued subpoena;
• state or local authorities within a specific state's juvenile justice system
• organizations conducting studies for, or on behalf of the school;
• accrediting organizations for accrediting purposes;
• specified officials for audit or evaluation purposes;
• parents of a dependent student;
• information designated as directory information;
• a parent of a student who is under 18 and not enrolled in postsecondary education;
• a student who has reached age 18 or enrolled in postsecondary education;
• in connection with a health or safety emergency.

An unauthorized disclosure occurs when personally identifiable information from a student's education record is made available to a third party who does not have legal authority to access the information.

An inadvertent disclosure occurs when information about an individual is unintentionally revealed through information released to the public. For example, through a security breach of an electronic records system or the result of an educator leaving paper reports in an unsecured location.
Understanding the law allows educators to act decisively and quickly when issues arise. "Balancing Student and School Safety: A Guide to the Family Education and Privacy Act for Elementary and Secondary Schools" is a helpful document from the Department of Education. We've included the PDF version in the attachments section of this presentation.

Congress enacted HIPAA, the Health Insurance Portability and Accountability Act in 1996 to protect the privacy and security of individually identifiable health information. The HIPAA Privacy Rule closely resembles the FERPA regulations, but for health information and records as opposed to general information.

Our main concern as educators is where FERPA and HIPAA Intersect.
When a school provides health care to students in the normal course of business, such as through its health clinic, it is also a "health care provider" as defined by HIPAA and required to protect patient/student health records.

However, many schools, even those that are HIPAA covered entities, are not required to comply with the HIPAA Privacy Rule because the only health records maintained by the school are considered "education records" or "treatment records" of eligible students under FERPA, therefore both are excluded from HIPAA requirements, yet refer back to FERPA.

A school that is not subject to FERPA and is a HIPAA covered entity must comply with the HIPAA Privacy Rule. For example, a private school not covered by FERPA that is a HIPAA covered entity must protect individually identifiable health information.

Requirements of IDEA, the Individuals with Disabilities Education Act closely resemble the FERPA statutes and definitions of "education records" and "personally identifiable information". As educators, there should be no misunderstanding that records maintained by a school subject to FERPA on a student with a disability receiving services under Part B of IDEA are "education records" subject to FERPA.

Like FERPA, The Protection of Pupil Rights Amendment (PPRA) applies to programs that receive funding from the U.S. Department of Education and is intended to protect the rights of parents and students in two ways:

• It seeks to ensure that schools and contractors make instructional materials available for inspection by parents if those materials will be used in connection with an Department of Education-funded survey, analysis, or evaluation in which their children participate; and

• It seeks to ensure that schools and contractors obtain written parental consent before minor students are required to participate in any Department of Education-funded survey, analysis, or evaluation that reveals information concerning:

- Political affiliations;
- Mental and psychological problems potentially embarrassing to the student or family;
- Sex behavior and attitudes;
- Illegal, anti-social, self-incriminating and demeaning behavior;
- Critical appraisals of other individuals with whom respondents have close family relationships;
- Legally recognized privileged relationships, such as lawyers, physicians, ministers;
- Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

The concept of privacy relates to individual autonomy and each person's control over their own information. This includes each person's right to decide when and whether to share personal information, how much information to share, and the circumstances under which that information can be shared.

Wherever ethics and the rule of law reside, unanswered questions and dilemmas are inevitable. With that in mind, the Department of Education has provided a valuable resource for providing those answers... the Privacy Technical Assistance Center or (PTAC).

The PTAC is designed to provide educators with a set of tools, resources, and opportunities to receive assistance with student privacy, security, and confidentiality issues and questions. It also acts as a means for states to share resources and best practices. State Education Agencies (SEAs), local educational agencies (LEAs), and postsecondary institutions can request, free of charge, on-site technical assistance for protecting their education data systems.

Questions concerning privacy, security, or confidentiality are too important to leave unanswered. The Privacy Technical Assistance Center Help Desk can be reached by email or phone:
PTAC Help Desk
PrivacyTA@ed.gov
Toll-Free 855-249-3071
The PTAC web address is www.ptac.ed.gov.