K-12 BLUEPRINT

A planning resource for personalizing learning

Everything You Always Wanted to Know About FERPA

toolkits

FERPA (Family Educational Rights and Privacy Act)

The Family Educational Rights and Privacy Act (FERPA) provides a set of rules for how schools can use and disclose education records. It protects the privacy of student education records and provides parents (and eligible students) with a set of rights, while requiring that schools provide notice to parents about those rights. According to FERPA, only a student's personally identifiable information (PII)—name, address, student ID, and other information that can link back to an individual—is protected. FERPA's definition of PII references "information, that alone or in combination, is linked or linkable to a specific student."

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. FERPA does, however, allow schools to disclose those records without consent to school officials with legitimate educational interest. Schools may share basic "directory" information, such as student names and addresses, if they give parents the opportunity to opt out. However, written permission is required to release all other student-level information if it is linked to any information that would enable a member of the school community to identify the student.

FERPA obligates schools to give parents certain access to their children's education records, and mandates these schools to determine whether or not a variety of third-party operators meet FERPA requirements for protecting student privacy with respect to data that is housed on their servers, applications, and software, and ensure that the operators are not accessing the data for other purposes.

Other FERPA issues include the following:

- Emergency situations (when and how to share data about people in distress)
- Responding to law enforcement requests for data
- Disciplinary records
- Vendor contracts and record keeping
- Record-keeping of data collected and disclosures

Enacted in 1974, FERPA was originally designed to protect the privacy of children's educational records and to prevent unwarranted disclosure. In February 2014, the U.S. Department of Education issued guidance for how today's schools and districts could apply this 40-year-old law to a world of metadata, digital learning tools, and data mining.

Legitimate privacy concerns are raised when a service provider has been granted access to a student's PII. According to the U.S. Department of Education, FERPA does not prohibit the use of cloud computing, but it sets the stage for schools—under the "school official" exception—to outsource to a cloud provider. This outside party must perform an institutional service for which the school would otherwise use employees, be under the direct control of the school with respect to the use and maintenance of education records, and be subject to requirements governing the use of PII from education records.

Currently, there is no statutorily approved method for de-identifying FERPA protected information. And with the abundance of online information available, it's a relatively simple process to "re-identify" individuals. In response, schools must negotiate stricter contractual terms with outside party providers regarding how metadata is collected and used. FERPA requires that records for a school be maintained separately—not mingled with data from other school systems or users—and that individuals employed by the provider may only access school records when necessary to provide the service to the school system.

With these considerations in mind, here are some questions to ask a service provider:

- Are the physical servers in a secured, locked, and monitored environment?
- How does the provider protect data in transit?
- Who has access to information stored or processed by the provider?
- Does the provider subcontract any functions, such as analytics?
- What is the provider's process for authenticating callers and resetting access controls, as well as establishing and deleting accounts?

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) to provide some guidance on the data security and privacy responsibilities of these providers, but has offered only limited enforcement in case of violations. Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices explains how schools and the companies and organizations they work with can meet FERPA compliance requirements. It recommends that schools:

- Maintain awareness of other relevant federal, state, tribal, or local laws;
- Be aware of which online educational services are currently being used in a district; and
- Have policies and procedures to evaluate and approve proposed online educational services.