
FOR YOUR INFORMATION

January 2010
News For School Clients

Authenticating the Identity of Recipients of Student Records

The federal Family Educational Rights and Privacy Act (FERPA) protects the privacy of student education records. School districts must abide by FERPA and its implementing regulations. Recently, the Department of Education (Department) amended the regulations in response to legislation, several United States Supreme Court decisions, advances in technology, increasing violence on school campuses, and other concerns about safeguarding the privacy of education records.

One important change relates to a school district's obligation to identify and authenticate the identity of the person to whom it discloses student records. The Department noted that parents and students have complained that unauthorized parties often obtain access to the student's education records because of a school district's failure to properly identify and authenticate the identity of the parents, students, school officials, and other parties to whom they disclose records.

The Department noted that identification of a party requesting disclosure of *hard copy* education records is relatively simple—the responsible school official can confirm the name and correct address for records sent by U.S. mail and obtain photo identification for records delivered in person. However, identification presents unique challenges in an *electronic or telephonic* environment where a U.S. mailing address is irrelevant and personal recognition or photo identification is not available.

The Department reported that unauthorized disclosures have occurred because schools provided access to records, either by electronic mail (e-mail) or by telephone, based merely on a requester providing widely available public information about the student, such as the student's name or date of birth. Such disclosures raised concerns about violations of FERPA, which states that a school district must not have a policy or practice of providing access to any personally identifiable information from education records without written consent or as permitted by law. The previous regulations did not address whether or how a school district must ensure that it has properly identified a party to whom it intends to disclose student education records.

In response to these concerns, the Department promulgated a new rule, 34 C.F.R. § 99.31(c). Under the new rule, school districts are required to use "*reasonable methods*" to identify and authenticate the identity of parties prior to any disclosure of education records. An example of an identifier for a student is the student's name or a unique identification number, such as the Wisconsin Student Number (WSN) or one issued by the school (most schools have ceased using social security numbers as student identifiers because of concerns about identity theft). E-mail addresses used by students to access or communicate in electronic systems may also be common, single identifiers.

Parents may provide districts with a telephone number or an e-mail address from which they can send and receive communications, which are considered single identifiers for the parents. The regulations address problems that arise when a school relies on widely available identifiers to both identify and authenticate the identity of the parent or other party requesting disclosure of education records.

Authentication of identity requires the district to ensure that the requester of student records, such as a parent, to whom it will disclose personally identifiable information is, in fact, the actual person entitled to access. The Department has stated that the use of widely available information to authenticate identity, such as reliance on the recipient's name or a student ID number, is not considered reasonable under the regulations. Authentication of identity can often involve requiring a user to provide information that only the user knows, such as a personal identification number (PIN), password, or answer to a personal question prior to disclosure of confidential student information.

The need to authenticate a person's identity can occur in a number of different situations where districts provide information electronically to parents, such as when communicating through e-mail. The school district must make sure (or authenticate) that the person sending the e-mail requesting information or with whom the district is sharing student information is actually the parent (or other person authorized to receive confidential student information). In other cases, parents may be seeking access to information, such as student grades or lunch accounts, through a computer database. Many districts provide the parent with a password to access the computer database. Use of a secret password in conjunction with a single identifier, such as the parent's

name, is one means of authenticating the parent's identity.

The regulations do not provide any specific means that a school district must take in order to ensure that it has "reasonable methods" in place to verify the identity of the person to whom they disclose records. Instead, the regulations allow a school district to use any reasonable method. Methods are considered "reasonable" if they reduce the risk of unauthorized disclosure to a level that is commensurate with the likely threat and potential harm. The "reasonableness" of the methods depend on a variety of factors, including the organization's size and resources.

Therefore, a school district may determine that "single-factor authorization," such as a standard form user-name combined with a secret PIN or password, is reasonable for protecting access to information such as electronic grades. A school may not make education records available electronically by using a common form user-name with a date of birth or social security number as an initial password to be changed upon first use of the system. The Department also stated that it expected that schools would deliver a password or PIN through the U.S. mail or in person. It also explained that "single-factor authorization" may not be reasonable for protecting access to information that could be used for identity theft and financial fraud, such as social security numbers.

Due to the differences in size, complexity, and access to technology, schools have the flexibility to decide what methods they will use to identify and authenticate the identity of recipients of student education records. In light of this new rule, it is advisable that school districts review their methods to make sure that they effectively reduce the risk of any unauthorized disclosure of education records.

If you have any questions regarding this topic, please call any of the following members of the Lathrop & Clark LLP School, Municipal, Labor and Employment Law Team.

Michael J. Julka (608) 286-7238
William L. Fahey (608) 286-7234
David E. Rohrer (608) 286-7249

Frank C. Sutherland (608) 286-7243
Joanne Harmon Curry (608) 286-7248
Shana R. Lewis (608) 286-7202

Richard F. Verstegen (608) 286-7233
Carrie M. Benedon (608) 286-7208
Todd J. Hepler (608) 286-7160

Disclaimer: Lathrop & Clark LLP provides this material as information about legal issues and not to give legal advice. In addition, this material may quickly become outdated. Anyone referencing this material must update the information presented to ensure accuracy. The use of the materials does not establish an attorney-client relationship, and Lathrop & Clark LLP recommends the use of legal counsel on specific matters.