

FERPA AND ELECTRONIC RECORDS: TEN DIFFICULT ISSUES TO CONSIDER

by

Patrick T. Andriano
Reed Smith LLP
Riverfront Plaza, West Tower
901 East Byrd Street, Suite 1700
Richmond, VA 23219
(804) 344-3426
pandriano@reedsmith.com

1. **Electronic records are not just found on computers**

Electronic information is found in a number of different locations. It can be found on multiple individual computers, servers, websites, cell phones, PDAs, voice mail, texts and in meta data. All of this information must be produced in response to a subpoena or preserved in response to a litigation hold notice. 34 C.F.R. Section 99.3.

2. **Producing electronic information in response to a subpoena or a parent's request is expensive and time-consuming.**

Fees may not be charged for searching for records. 34 C.F.R. Section 99.11(b). Fees may be charged for copies if the charge will not prevent the parent's right of access. 34 C.F.R. Section 99.11(a). There is a need for gathering data in a thoughtful and systematic manner. Compile a list of personnel who would have records in their possession. Notify them of the litigation hold. Consult with Information Technology personnel to prevent inadvertent destruction of information. Carefully consider search parameters. It is necessary to redact information regarding other students or privileged information prior to producing. 34 C.F.R. Section 99.12.

3. **Your private electronic information may be subject to discovery if you use your personal computer, cell phone or PDA for work.**

Those who work in the public sector are governed by FERPA, HIPAA, and FOIA. Also, check for any state statutes or regulations dealing with disclosure of student information. Information that cannot be obtained in another manner may be subject to a subpoena. Never assume that any record you create is exempt from disclosure. Write and send communications only if you are content to have it released to the parents or to the newspaper.

4. **Try to reduce the school district's electronic footprint.**

Records are located in so many different places that it is increasingly more difficult to gather these records if they are in electronic form. Try to limit the number of locations in which records are stored. Make staff aware of the locations they should advise parents to visit in order to locate records. Advise staff to try to stop utilizing email. It is perfectly permissible to speak in person or by telephone. Oral communications which are not recorded are not records and need not be produced.

5. **Penalties for non-compliance with the litigation hold requirements can be large.**

See the discussion in *Pens. Comm of the Univ. of Montreal Pens. Plan, et al., v. Banc of Am. Sec. LLC*, 685 F.Supp.2d 456 (S.D.N.Y. Jan 15, 2010). There is, however, no private cause of action by parents for a FERPA violation. *Gonzaga University v. Doe*, 536 U.S. 273 (2002).

6. **The security of electronic information must be insured by the school district.**

A school district must protect confidential information at multiple stages: collection, storage, disclosure and destruction. 34 C.F.R. Section 300.623. There must be one individual who is designated to be in charge of ensuring confidentiality. Staff must have training regarding the collection and use of personally identifiable information in accordance with state policies and procedures. Think before forwarding communications by e-mail or facsimile. Has this method of communication been specifically approved by the parents or will it result in an unlawful disclosure?

7. **Be aware of automatic email clean up practices.**

Many school districts have a policy whereby electronic information of a certain age is automatically deleted. Be cautious and consider whether this destruction must be mentioned in the annual FERPA notice.

8. **Records cannot be destroyed without notice to the parents.**

Generally, records are maintained until no longer needed, but must be maintained for not less than five years. There does not appear to be an exception to this practice for electronic records. In Alaska, destruction of records cannot occur sooner than 45 days after the date of the notice to the parents.

9. **Check for state law issues.**

Alaska appears to require a disclosure of records within 10 business days and the provision of copies of records to parents. It is to be assumed that parents have a right of access to their child's records. Maintain a list of persons authorized to have access to personally identifiable information. Maintain lists of the training provided to staff, attendees and subjects covered. Blank protocols are not educational records. Completed protocols are educational records to which parents have a right of access.

10. **Create an electronic records policy.**

Such a policy should address permitted uses, right of access by employer and define the type of information that is "officially" maintained regarding a student. The policy should also provide for a procedure, which includes a hearing, to challenge the accuracy of records, whether they are misleading, and whether they violate privacy or other rights.