FERPA and the MGDPA:
What Faculty and Staff Need to Know About Handling Education Records

Minnesota State University Mankato
October 6, 2004

Kris Kaplan, Assistant General Counsel
Minnesota State Colleges and Universities Office of the Chancellor
Kristine.kaplan@so.mnscu.edu 651 296-3905

I. What *is* FERPA anyway?

The Family Educational Rights and Privacy Act (FERPA)

- Federal law that regulates how all schools that accept federal funds handle "education records."

The Minnesota Government Data Practices Act (MGDPA) adds requirements in handling all government data, including education records (a.k.a. "educational data.").

II. Why Do I Need to Know About FERPA?

It's the law – and has been since 1974. State employees who create and handle education records every day must understand their roles in maintaining education records in accordance with federal and state data privacy laws.

Violations of data privacy laws expose the school *and individuals* to liability.

- Illegal FERPA policies could result in withdrawal of federal funds to the university.
- Under the MGDPA, institutions can be liable for money damages, or civil penalties, and *individuals* are subject to disciplinary action for willful violations, and potentially even criminal penalties.

Moreover, it is important for the integrity of the MnSCU system that we honor students' rights to access and maintain privacy in the education records that are entrusted to us.

III. What are "Education Records"?

"Education records" are data maintained by the school (or an agent or employee acting in his/her official capacity) that directly relate to an individually identifiable student.

- Very broad – not just the "official file."
- May be in *any tangible (including electronic) media or form*.

- Includes admissions materials, financial aid records, transcripts, class lists, class schedules, graded exams or papers, records of disciplinary proceedings, photographs, work study records and much more.

Certain information is exempted from the definition of "education record"

- "Sole possession" notes of instructors;
- Law enforcement unit records – not shared with school officials and maintained for law enforcement purpose;
- Alumni records – information about individuals when no longer students;
- Medical treatment records – only accessible by treatment providers.

The privacy rules applicable to such records will vary.

IV. How Do Privacy Laws Classify Education Records?

Most education records are "*private*" as to the subject student, which means:

- Accessible to the student.
- Accessible to others at institution who have a legitimate educational interest.
- Accessible to third parties *only* with written consent of student or as otherwise authorized by law.

"Directory Data" is *public* and available to anyone.
Directory Data is defined differently at each school. *Some information is NEVER public: SSN, Student ID Number, race, ethnicity, gender and similar information.*

Directory data at MSUM is defined as:

- Name; local and permanent address(es) and phone number(s);
- E-mail address
- Date and place of birth
- Program/major field of study
- Class status (freshman, sophomore, etc.)
- Degree, honors and awards received
- Participation in officially recognized activities and sports
- Weight and height of members of athletic teams
- Dates of attendance
- Most recent previous educational agency or institution attended

Don't automatically assume you can release directory data. *Students have the right to refuse the disclosure of their data. This must be honored in all contexts – not limited to omission from student directory.* Consult the Registrar for information on whether students have "opted out."

Be careful about releasing directory data that indirectly reveals private information. E.g., school officials could not respond to a request for a list of names of "all African American computer science majors" even though names and majors are "directory."

V. What Rights Do Students Have in Their Education Records?

The primary rights:

- To inspect and copy their education records.
- To request to amend an education record if inaccurate or incomplete.
- To have some control over disclosure of education records.
- To file a complaint with the FERPA Office in Washington D.C.

In Minnesota, students' rights in their education records begin upon application and generally continue post-attendance (private data remains private after student leaves).

All students in higher education have the same rights regardless of their age.

International students have the same privacy rights except that the CIS (f.k.a. INS) gets access to certain information without specific consent.

VI. Who Has Access to Education Records Other Than the Student?

- Anyone with *prior, written consent* of student.
- Anyone asking for d*irectory data* unless
  - Student has "opted out" (see above).
- *"School officials"* who have a "*legitimate educational interest" in those records.* Each school defines, at MSUM means:
  - A *school official* is a person employed by the university in an administrative, supervisory, academic or research or support staff (including a school's law enforcement unit personnel and health staff); a person or company with whom the university has contracted (such as an attorney, auditor, or collection agent); a person serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.
  - A school official has a *legitimate educational interest* if the official needs to review an education record in order to fulfill his or her professional responsibility; i.e., "need-to-know."
- Third parties as authorized by law, e.g.,
  - To comply with a valid subpoena or judicial order (after notice to student)
  - To assist in health or safety *emergency* (narrow definition – imminent risk of physical harm).

VII. What are the Rights and Responsibilities of Faculty and Staff Regarding Education Records?

A. Respect Appropriate Limits on Access by School Officials

State employees have a legal responsibility to protect the privacy of student educational records under their control, including access within the institution.
Need-to-know is the basic principle.

Limit your access to what is necessary for your work – your technical ability to access data may be broader than your legal authority.

If you are not clear about another employee's right to access student information, ask them to explain. Curiosity is not a "legitimate educational interest." Limit the disclosure to what is really necessary to perform the job.

Be careful about inappropriate re-disclosure – including inadvertent viewing on desktops or computer screens or oral disclosures to colleagues who don't have legitimate educational interest.

B. Know Your Resources

Keep copies of applicable policies/procedures handy
- Annual notice to students of rights
- Public access policy
- Policy on charging for copies
- Other?

Know who to call for assistance – every campus has a **Data Practices Compliance Official** who can help answer questions. At MSUM: Carol Stallkamp.

C. Provide Appropriate Collection Notice

Collect private data only as necessary. Restrict use of SSN or other personal identifiers.

When collecting private data from students, must give **Data Practices Notice ("Tennessen Warning"):**
- Why the data is being collected – how used
- Whether legally required to provide
- Consequences of refusing or supplying
- Who may have access
- For SSNs - legal authority to request

Notice may be oral, but written is better record.

D. Maintain Securely

Keep private data secure – the laws apply to your handling of data wherever located.
- If you need to take private data home, do not allow improper disclosure to family or others

- Follow IT security standards for encryption, etc.

In the workplace
- Guard views of private data on your computer screen
- Don't "over-expose" private data by leaving it out unnecessarily

Social security numbers and medical data especially sensitive.

No portion of student's SSN may be used for public identification, including, for example, posting of grades.

E. Release Appropriately

Before releasing data on one student always check to be sure it doesn't improperly contain data on others.

To **students** who are subjects of data (*under MGDPA within ten working days*). Laws do not require written request – MSUM FERPA Notice suggests that students submit written request to appropriate school official who maintains records.

To **parents**:
- With prior, written consent of student; or
- In health or safety *emergency* (a narrow exception – consult Data Privacy Official if possible).

To **third parties** – e.g., press, unions, law enforcement, other students, potential employers:
- **Prior, written consent** of student generally required that meets the following standards:
  - Specifies records to be released
  - States purpose of disclosure
  - Identifies person(s) or class of persons to have access
  - Is *signed* and dated

A release that does not include all the above requirements is not valid and cannot be honored. If that happens, provide a substitute, valid form.

A **sample release** is available on MnSCU Office of General Counsel Web site: www.ogc.mnscu.edu.

A faxed release, if signed and dated is ok;
An e-mail "authorization" is not ok – need *signature*.
Electronic signatures were recently approved for giving written consent where required under FERPA, but stringent standards must be met.

To third parties **without consent as authorized by law**. e.g., to organizations auditing school programs or financial aid; for health or safety emergency (imminent danger required); in response to valid subpoena or court order, and other exceptions:

- Disclose only what the law authorizes;
- Maintain appropriate records of disclosure
    - Who, what, when – keep with student's records.

If in doubt, consult – in almost every case immediate response is not required.

Always refer legal process or law enforcement requests to DPCO. *Responding to court orders or subpoenas requires special procedures, including notice to student, in most cases. Child support enforcement officials must obtain subpoena for private student data.*

VIII. Procedures for Responding to Requests from Third Parties for Private Information on Students.

Consult school policy/procedures for whether written request required and whether/how to charge for copies of information, if requested.

In person

If served with a **search warrant**, obtain ID of official and a copy of the warrant; cooperate with search and notify the OGC or AGO as soon as practical.

In other cases: Ask for student's written release – check to make sure it complies with requirements described above; ask for ID of requesting party.
If no release, may provide only directory information (so long as student hasn't "opted out") unless there is specific legal authority to release.
If legal authority is claimed, ask what it is and for a copy of the law, if possible. Limit disclosure to what the law requires – government officials who need more can obtain subpoenas.
If a **health or safety emergency** is claimed, establish reasonable basis that there is *imminent danger of physical harm* to the student or others – if not, do not give out private data (including class schedules or locations) but may agree to appropriate assistance.

By telephone

- **Call from student –** may provide private data to student so long as you make reasonable attempt to verify identity.
- **Call from third party –** may only provide public "directory data" unless have written release from student. Remember to verify that student has not restricted release of directory data. If you have release, may provide only private information that is authorized. Verify the caller's identity.

By fax or e-mail

Sending private data by these means is arguably more risky than U.S. Mail as you have less assurance of who has access at the receiving end, especially to third parties. Take

reasonable security precautions, including following any IT standards regarding electronic transmissions. May call to verify fax receipt.

Using a Web site to disseminate private student data
It is acceptable for students to access *their own* data by use of a confidential PIN number on a secure Web application.

X. Special Topics for Faculty

A. References

Always advisable to get student's prior written release (see elements above) even if not technically releasing private data. A sample form is attached and available on MnSCU Office of General Counsel Web site: www.ogc.mnscu.edu.

- A faxed release, if signed and dated is ok
- An e-mailed "release" is not ok – need *signed* release.

Even if student has requested "reference," cannot assume you have consent to release private data like grades, or GPA. So, clarify – in writing. Get a release.

To avoid potential defamation claims, stick to facts and opinions based on facts.

If you want reference to be confidential, student may be asked to waive right to see – will be valid even if student changes mind later. But student cannot be required to waive.

If you're not sure your reference would be helpful to student, review with him/her what you feel comfortable saying and let the student decide whether to send.

B. Responding to requests for information on students:

It is always safest to try to stick with a policy of responding only to written requests and only in writing. However, that may not always be practical.

By telephone

- **Call from student –** may provide private data to student so long as you make reasonable attempt to verify identity.
- **Call from third party –** may only provide public "directory data" unless have written release from student. If you have release, may provide only private information that is authorized. Verify who you are speaking to. *Remember, there are no "off-the-record" comments.*

By fax or e-mail

- Sending private data by these means is arguably more risky than U.S. Mail as you have less assurance of who has access at the receiving end, especially to third parties. Take reasonable security

precautions, including following any IT standards regarding electronic transmissions.

C. Electronic Privacy in the Classroom

Can faculty legally use e-mail to communicate with students? Sure, but remember any tangible form of communication for "official" purposes will probably be considered collection and creation of education records, and so the applicable privacy rules will apply. Be cautious about sending "sensitive" information electronically. Best practice is not to send private data electronically unless encrypted. Consult campus IT to understand security issues.

May faculty share students' e-mail addresses with other students? Since e-mail addresses at MSUM are directory data this would not be a problem so long as students' rights to "opt out" are honored. Students who wish to suppress their directory data should be allowed an alternative means of communication if possible. If faculty intends to use e-mail or electronic communication tools for required classroom participation, they should include such information in the syllabus to alert students who may wish to seek out other sections.

Is it acceptable to use a Web site to disseminate private student data?
It is acceptable for students to access *their own* data by use of a confidential PIN number on a secure Web application.

Be sure to work with your IT personnel to build in the necessary security measures.

Want more information on Data Practices issues?

See the MnSCU Office of General Counsel Web site:
www.ogc.mnscu.edu .