Legal & Student Data Privacy Issues

Susan Van Voorhis
Registrar
612-625-8098

Tracy M. Smith
Associate General Counsel
612-624-9546
Laws governing data and data privacy

- Minnesota Government Data Practices Act
- Family Educational Rights and Privacy Act (FERPA)
What is FERPA and to whom does it apply?

- Purpose is to protect the privacy rights of student educational records and to ensure the accuracy of those records
- Applies to currently enrolled or formerly enrolled students (regardless of age or parental dependency status)
- Applies to all institutions that receive federal funds
What is the MGDPA?

- Minnesota Government Data Practices Act (MGDPA) prescribes specific requirements for handling government data, which includes “educational data”
- Applies to all public institutions – including U of MN
- Applies to applicant data
- For individuals’ request for data about themselves, need to respond within 10 working days
What rights does FERPA afford students?

- Right to inspect and review the record (all parts with two exceptions: letters of recommendation where student has waived right of access, and parents’ financial info)

- Right to request an amendment to the record that the student believes is inaccurate or misleading or violation of his/her privacy rights (recording error not substantive decision) and to request a hearing if request to amend is not granted

- Right to consent to disclosure of personally identifiable information
What rights does FERPA afford students?

- Right to know what institution has designated as public/directory information and the right to request suppression of their public/directory information.
- Right to know that school officials may access their records and the criteria for determining that a school official has a legitimate need to know the information.
- Right to file a complaint with the Family Policy Compliance Office in the U.S. Department of Education.
What are education records?

- Any record from which a student can be personally identified AND which is maintained by the institution regardless of its form (e.g., handwritten, print, database, disk, email, files, graded materials, class lists, individual student class schedules, financial aid records)
- Includes notes, emails, any other record
What is directory/public information?

- Information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed.

- FERPA allows each school to choose what information is public/directory – can choose nothing – ours decided by the Board of Regents.
What is directory/public information at the U of MN?

- Name
- Address
- Email address
- Telephone number
- Dates of enrollment
- Enrollment status (full/part time, not enrolled)

- Major
- Adviser
- College
- Class (freshman, sophomore, etc.)
- Academic awards and honors
- Degree(s) received

* Other information is private
What cannot be considered directory information?

- Grades
- GPA
- Race
- Gender
- Social Security Number
- Country of citizenship
- Religion
Directory information use/release?

- Must allow students opportunity to limit release (suppress) public data – look for “window shade” icon in PeopleSoft.
- If the information is public, and not suppressed, we must release it – check for suppression before releasing.
- If you can see the information on the on-line University directory, it is non-suppressed public information and can be released.
- Provide copies of information – except parents’ financial and waived letters of recommendations – upon request.
Who has access to student’s education records?

- The student (always has access with the two exceptions mentioned)
- Any outside party that has the student’s written consent (get a copy of the consent)
  http://www.ogc.umn.edu/faq_info4.html
- Parents of financially dependent students (per last tax return)
- Any appropriate person in health or safety emergency
The “health and safety” emergency exception is for sharing information outside the University. Sharing within the University is less restrictive – but still requires legitimate educational interest.

Can disclose information to “appropriate parties” in connection with an “emergency” if necessary to protect “health or safety” of student or others.

“Appropriate parties” could include student’s doctor, police, parents, etc.

“Emergency” is not further defined. Need not hold ourselves to standard of clearly imminent harm. Use best professional judgment to determine what is appropriate to protect student or community.

“Health or safety” can mean protecting student’s physical or mental health (e.g., eating disorders, suicidal tendencies, delusional thinking) or safety of the student or community (e.g., violent tendencies, student is missing, etc.).

OGC frequently advises on health or safety questions.
Who has access to student’s education records?

- The student (always has access with the two exceptions mentioned)
- Any outside party that has the student’s written consent (get a copy of the consent) http://www.ogc.umn.edu/faq_info4.html
- Parents of financially dependent students (per last tax return)
- Any appropriate person in health or safety emergency
- School officials with legitimate educational interest
What is a school official?

- Members of the institutional community who act in the student’s educational interest within the constraint of their need to know.
- Generally, someone the institution has employed, contracted with, or has other official relationship with who would need to access pertinent student data to perform their designated job functions.
What is legitimate educational interest?

- Often referred to as “need to know”
- Interest in reviewing student education records for the purpose of performing assigned institutional research, educational or administrative function
- Guiding principle – If you need the data to perform your job duties you should have access to it
Examples of legitimate educational interest

- Disruptive behavior in classroom or disturbing writings or comments – may share with Dean’s Office, UMPD, Boynton, University Counseling, Disability Services, Behavioral Intervention Team (Office for Student Conduct & Academic Integrity) or others within the University who may help resolve the student’s issues or protect the community.

- Student who is student-athlete and a Housing resident is transported by UMPD to the hospital for detox and making suicidal comments – Housing and Athletics and others have a legitimate educational interest in knowing about the health concern for this student.

- Not every school official has a “legitimate educational interest” in every circumstance (e.g., there is no need to offer information about a housing violation to all of a student’s instructors) – use judgment – what is the purpose of disclosing the information?
What not to collect or store

- Social Security Number
  - Do not collect or use SSN unless absolutely necessary
  - If using or collecting SSN must use a secure server, registered with OIT or store in a secure physical location
  - If collecting SSN, must give a reason it is being collected and how it will be used – “Tennessen Warning”
  - Must shred any information containing a SSN – look at old forms

- Health information
  - Do not collect health information unless absolutely necessary
  - Must shred when no longer necessary
What can we do to ensure privacy?

- Destroy Information as applicable
- Properly destroy information
- Properly secure information
- Properly secure belongings
What if you inadvertently release private data?

- Notify your supervisor
- If possible, remove the material from public view
- Submit the concern to abuse@umn.edu
- Must report breaches of security to OIT Security and Assurance via abuse@umn.edu