January 14, 2021

Office of General Counsel

Basic Data Practices Overview

Daniel McCabe
Assistant General Counsel

Part One: Classifying Data

Public Data

- Default rule under MGDPA – Government Data is Public
- Available to inspect upon request
- Examples include contracts, invoices, policies, and most business correspondence
- Data Classification: Low

Private Data

- Certain data sets are private under the MGDPA/FERPA
- Data Classification: Restricted or Highly Restricted
- Private means accessible only:
  - to data subject
  - for work related purposes
  - to third parties (who are not the data requestor themselves) if:
    - Subject gives consent or;
    - Appropriate legal authority, such as a court order

Personnel Data

- Section 13.43 sets forth what is Public Data on Employees
  - Only data listed in 13.43 is public data
  - If an employee asks for data on themselves, they receive that data whether it is public or private in most circumstances
  - **Otherwise, Personnel Data is Private**

General Exceptions

- “Security data” rule allows College to withhold otherwise public data if disclosing the data may jeopardize the security of the College or an individual
- “Trade secrets” remain confidential information
- Labor Relations Data
- Employee Parking spaces

Identifying Educational/FERPA Data

- "Educational Data" means (almost) all data relating to a student.
- Educational Data is generally private data. This means that it cannot be disclosed without the student's written consent unless an exception applies.
- Educational Data remains private after a student is no longer enrolled due to graduation, transfer, etc.
- Educational Data does not include data collected after a student leaves the college (e.g. alumni data).
- "Directory Data" is public, unless a student asks that it remain private.

Zoom and FERPA

- FERPA does not allow a student to remain anonymous in the classroom.
- The System's contract with Zoom limits what Zoom can do with the recordings to remain FERPA complaint.
- No system employee (faculty, staff) should share the videos outside the class itself.
- If an individual faculty member wants to privatize student identities, Zoom allows them to do so. This is optional.

Directory Data

- Public data under the MGDPA.
- Each campus has their own definition.
- Learn your campus' definition.

Limited Directory Data

- Data you can define as disclosable to specific third parties for specific reasons.
- STAR IDs and email addresses may be shared internally for providing services and technical support to students, and for publication in the online Student Directory and inclusion in the Office 365 Global Address List.
- Student contact information to student associations.

Using Images

- “School Officials” (including designated contractors)
- Transfer exception
- Certain Federal or State programs
- Financial aid exception
- Accreditation
- Health or safety emergency
- Solomon Amendment
- Certain disciplinary proceeding purposes
- Records with no personally identifiable data
- Research exception
- There are other exceptions. If you are not sure if an exception applies, ask the Data Practices Compliance Officer.
- “Test” exception
- Student resident information to local elections boards

Non-FERPA Student Records

- "Sole-Possession" records:
  - Faculty's instructional notes, not shared with anyone except substitutes, destroyed at the end of the semester;
- Records created and maintained by the school's law enforcement division, if there is one;
- Employment records for non-Federal Work Study student employees;
- Alumni records and other records created after graduation.
- Records created before a prospective student applies.

Internal Data Use - Work Purposes

- You can only utilize non-public data for legitimate work purposes.
- “Legitimate Educational Purposes” is not all encompassing. For example, the Financial Aid Office may have a legitimate interest in student financial records, but a student’s academic advisor may not. This is situation specific.

Part Two: Managing Data

Internal or External Request – Questions to Ask Yourself

- For internal requests, does this person have a business need to access the information?
- For external requests, is the person the data subject? If not, is the data public or private?

Response Time and Multiple Requests

- Keep in mind that only Data Practices Compliance Officials are responsible for fulfilling data requests.
- If someone is asking for their own data – 10 business days.
- Otherwise, we have a “reasonable” time to respond.
- A data subject cannot ask for the same data twice in a six month period.
- A member of the public who is not the data subject can ask for data as many times as they want.
- These restrictions still exist despite the status of our operations.

Asking for More Information

- We cannot:
  - Ask for data requestor why they are asking for data
  - Ask data requestor to identify themselves, unless they are asking for data on themselves
- We can:
  - Ask to clarify a request
  - Ask for requests to be in writing
  - Ask a data requestor for identification if they are asking for data on themselves
  - Ask if a data requestor is a credit card issuer

Identity Verification

- Persons are entitled to government data on themselves in most circumstances.
- However, we have to verify that someone is who they say they are when they ask for “data on themselves.”
- Reasonable procedures include making the person come to an office and present photo identification or using a verifiable portal such as “Move-It Securely” or D2L.
- In person verification is not currently an option, so we should consider how we remote verify.

Valid Releases

- Must be *signed* and dated by data subject.
  - Must sufficiently describe the information to be released and to whom it is to be released to.
  - May be a category such as “future employers” but specific names preferred.
  - Fax copy ok but e-mail alone is not.
  - Requests for data authorized by the data subject must be fulfilled within ten (10) business days. This is the same timeline as if the request came from the data subject themselves.

Record Retention and Storage

- Government data must be kept in a manner that is readily accessible for convenient use.
- Files should be well organized with easily understood labels.
- Follow record retention policies. HR, Finance, and Facilities records fall under Statewide General Schedules, and campuses typically have their own retention schedules for other documents.
- In addition, there is a requirement to maintain a “data inventory.” This is separate from System Office IT’s data classification project.

Data Breaches

The MGDPA requires notice to affected individuals of a breach of security (unauthorized access) for

- any private or confidential data (not just SSN or financial information)
- in any medium (not just computerized).

E.g., lost or stolen laptop containing student program data.

Contact your supervisor or campus DPCO if you believe you have a possible security breach situation.

- OGC will assist in determining whether notice is required, how it must be done and other details.

THE FEDERAL DEPARTMENT OF EDUCATION NOW REQUIRES SAME-DAY NOTIFICATION OF DATA BREACHES.

Data Collection: Tennessen Warning Notice

- The reason government is collecting the data,
- How government plans to use the data,
- Whether the person is legally required to provide the data or may refuse to do so,
- Consequences if the person provides the data,
- Consequences if the person does not provide the data, and

Data Collection: Tennessen Warning Notice

- The identities of people and entities that have access to the data by law. (For example, all notices should include that data may be shared upon court order or provided to the state or legislative auditor.
- Note regarding private data on minors: Entities must provide minors with notice that they have the right to request that parental access to private data be denied. Entities may consider including this notice in the Tennessen Warning notice when collecting the data (See Minnesota Rules 1205.0500).

Consequences of Violations

- A violation of the Data Practices Act could result in:
  - Court order for corrective action
  - Damages to data subject
  - A violation of Section 13.32 (FERPA) could result in sanctions by the Department of Education

Data Practices Compliance Officers

- Responsible for MGDPA/FERPA compliance, responding to MGDPA requests, and answering questions about access to public data.
- DPCO's are not required to answer questions about the data itself.

Part Three: Scenarios

Scenarios

- One of your employees reports that a College owned laptop was stolen out of their car. What needs to be done?
- One of your employees reports that they were able to open up a screen that showed employee home addresses and dependent information that they haveno business reason to see. What should you do?
- One of your employees used a personal computer instead of a work-issued one to do work at home. Is this okay?

Scenarios

- Your department is moving. You want to clean out your file cabinets and throw away what you no longer need. Can you?
- You supervise a large department that works in several locations. To assist in identification, you want to post employee photos on a bulletin board along with their names and some “fun facts” that the employee chooses to submit. Is this allowed?

Scenarios

- A student asks for a copy of their high school transcript. They refuse to tell you why, but they agree to pay for the copy costs. Can you provide it to them?
- A faculty member asks for a student's transcript in order to write that student a recommendation. What should the College do?
- A parent asks to see their child's grades. The student is a PSEO student and a minor. What should the College do?

Scenarios

- An external law enforcement agency asks for a student's schedule. Under what circumstances can you provide this information?
- A recruiting company wants student email addresses in order to contact them about job openings. Should you provide this information?
- A parent comes to class and asks questions about a student's progress and how to help the student complete assignments. What should the faculty member provide?

Scenarios

- You remember when students graded each other's pop quizzes. Is this a FERPA violation?
- A high school counselor asks for information on a student that has applied to the College. What information can you provide the counselor?
- You take notes observing students in your clinic. You share the notes with the director. These are your private, handwritten notes. Are these notes covered by FERPA?

Scenarios

- A student keys your car, so you make a conduct complaint. You are told by your supervisor that are not allowed to review the conduct case because you do not have a legitimate educational purpose to access it. Is this correct?
- A student on an honors evaluation committee needs access to another student's educational records. You feel the student is a "school official" so you provide access. Can a student be a "school official?"
- A student commits an infamous crime. A reporter asks you some questions about how he did in school. The reporter says that since the student is now a "public figure" you can provide this information. Is the reporter correct?

Minnesota State Contact Information

Dan McCabe
Assistant General Counsel
daniel.mccabe@minnstate.edu
651-201-1833

Office of General Counsel
https://www.minnstate.edu/system/ogc/index.html

Questions and Answers

- Please chat in your questions to the host.

How to Access Today's Materials

- Within a few business days, the recording link and PDF will be available

OR

- If you would like a PDF copy of the PowerPoint right away, contact Liz Hegman at liz.hegman@minnstate.edu