Basic Data Practices Overview

Daniel McCabe, Assistant General Counsel

Office of General Counsel

September 11, 2025

Presentation Overview

- Part One: Classifying Data
- Part Two: Managing Data
- Part Three: Data Sharing with Foundations

Part One: Classifying Data

Data Practices Laws

- Minnesota Government Data Practices Act (MGDPA)
- Family Educational Rights and Privacy Act (FERPA)
- HIPAA, GDPR, etc.

Public Data

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

Private Data

- Certain data sets are private under the MGDPA/FERPA
- 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
  - The list includes salary, job title, job description, name, office contact information, existence and status of complaints, etc.
  - 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 Minnesota State to withhold otherwise public data if disclosing the data may jeopardize the security of Minnesota State, Minnesota State property or an individual.
- Trade secrets
- 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 alumni or prospective student data.
- "Directory Data" is public, unless a student asks that it remain private.

Directory & Limited Directory Data

- “Directory Data” is public data under the MGDPA.
- Students can “suppress” directory data upon request. This makes it PRIVATE.
- “Limited Directory Data” is only public for specific purposes.

Other FERPA Exceptions

- "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 (e.g. crimes of violence)
- Records with no personally identifiable data
- Research exception
- "Test" exception
- There are other exceptions. If you are not sure if an exception applies, ask the Data Practices Compliance Officer.

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.

Treatment Records

- Student health records are governed by FERPA, not HIPAA (Joint Guidance).
- “Treatment Records” are a special definition under the Joint Guidance. These records are only available to treating professionals.
  - If Treatment Records are shared with non-professionals, they lose that status (but are still protected by FERPA).
  - The MGDPA requires disclosure of private data to a data subject.

Part Two: Managing Data

Record Retention and Storage

- Government data must be kept in a manner that is readily accessible for convenient use.
- Follow record retention policies.

Internal or External Data Sharing – 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?

Responses to Data Requests

- Data Practices Compliance Officials are responsible for fulfilling public data requests.
- If someone is asking for their own data – 10 business days. Including student data (shorter timeframe than FERPA).
- Otherwise, we have a “reasonable” time to respond.

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 private data on themselves
  - Ignore a data request, even if it's from a personal email address
- 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 (if asking for student names or contact information)

Identity Verification

- Persons are entitled to government data on themselves in most circumstances.
- However, we must 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.
- We can also ask people to show their photo ID on a video call.

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 and for what purpose.
  - May be a category such as “future employers” but specific names preferred.
  - 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.

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.

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

Data Collection: Tennessen Warning Notice (2)

- 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 paid to the data subject
  - A violation of FERPA could also result in sanctions by the Department of Education
  - Failure to comply with job requirements
  - Reputational damage to the University

Part Three: Sharing Data with Foundations

Foundation Operations and Minnesota State

- We have separate foundations mainly for fundraising purposes (with some narrow exceptions).
- The colleges and universities contract with the foundations to fundraise and manage funds.
- The foundations contract with the colleges and universities to provide administrative services.
- The foundations, however, are separate legal entities.

When Can Colleges and Universities Share Data with Foundations?

- Private, non-student data
  - Is the foundation performing a task for the College or University?
  - Does the foundation need the data to perform that task?

Note: Private data cannot be shared for a foundation-only task (e.g. fund management).

When Can Colleges and Universities Share Data with Foundations? (2)

- Student Data
  - Is the foundation a school official with a legitimate business need to access the data?
  - Is the data limited directory data for sharing with the foundation or directory data?

Contact Information

Dan McCabe

Assistant General Counsel

daniel.mccabe@minnstate.edu

651-314-3428

Please Take Our Survey

A link to the survey is in the chat. Please provide your feedback.

Questions and Answers

Please chat in your questions.

Thank you.

MINNESOTA STATE

30 East 7th Street, Suite 350
St. Paul, MN 55101-7804

651-201-1800
888-667-2848

MinnState.edu