October 10, 2019

Office of General Counsel

Minnesota Government Data Practices Act

Daniel McCabe

Assistant General Counsel

MINNESOTA STATE

Public Data

Default rule under MGDPA – Government Data is Public

- Available to inspect upon request
- Copies available – we have an option to charge according to the MGDPA's guidelines
- Examples include contracts, invoices, policies, and most business correspondence

Private Data

Certain data sets are private under the MGDPA

- "Private" means:
  - Accessible to subject within 10 business days
  - Accessible to our employees or agents for job-related needs
  - Accessible to third parties with:
    - Subject's written (signed, dated) consent, or
    - Appropriate legal authority.
- Social Security Numbers are always private.
- Collect, maintain only what is needed.

Internal or External Request

- 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

- 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

Asking for More Information

We cannot:

- Ask a data requestor why they are asking for data
- Ask a 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
- We can ask a data requestor if they are a credit card issuer if the request is for student contact information.

Copies

Members of the Public who are Not the Data Subject

- If the request is for 100 or fewer pages of black and white, letter or legal sized paper copies, the maximum allowable charge is 25 cents for each page copied, or 50¢ for a two-sided copy. This charge is a flat rate; government cannot add on any additional charges, such as cost of mailing or paper.
- For copies of other data (more than 100 paper copies, photographs, data on a CD or DVD, data stored electronically, etc.) government may charge the actual cost for an employee to search for and retrieve the data, and to make paper copies or to print copies of electronically stored data.

Copies (2)

Data Subjects

- Government may charge the actual cost for an employee to make paper copies or to print copies of electronically stored data. Government may not charge a data subject any fee for searching for and retrieving data (Note that the 25 cents per page per 100 copies or fewer does not apply to data subject requesters unless that is the actual cost to make copies.).
- We cannot charge if someone wants to come in an “inspect” data

Record Retention and Storage

- Government data must be kept in a manner that is readily searchable for convenient access.
- 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 have their own retention schedules for other documents.
- In addition there is a requirement to maintain a “data inventory.”
- System data classification policy also classifies different data sets using “public,” “restricted,” and “highly-restricted” classifications.

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.”

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.

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
- 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).

13.43: Public Data on Employees

Section 13.43 Sets forth what is Public Data on Employees

- Only data listed in 13.43 is public data.
- Only give what is being requested.
- If an employee asks for data on themselves, they receive that data whether it is public or private in most circumstances.

13.10: Decedents

- Private data on decedents remains private when ten years have elapsed from date of death and thirty years have elapsed since the creation of the data.
- FERPA protections do not extend beyond death, but 13.10 protections do.

13.37: 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

FERPA and MGDPA

- FERPA is codified in Section 13.32 of the MGDPA.
- Both deal with student “Educational Data.”
- There are differences:
  - Students, can access their data within ten (10) business days, a shorter time period than the default under FERPA.
  - If a student agrees to pay copy costs, we must provide copies of their data.
  - FERPA protections begin at application, not at registration.
  - Directory Data is public.

Identifying FERPA Protected Data

Educational Data is Protected by FERPA

- "Educational Data" means 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).
- Educational Data can be utilized by School Officials for legitimate business purposes.

What is a Student?

A “Student” is defined in the MGPDA as:

- Individual currently or formerly enrolled;
- Applicants for enrollment; or
- Individuals who receive time shared educational services.

What is a School Official?

Schools officials have access to Educational Data for legitimate business purposes.

- This can include contractors, students, or anyone else performing a duty for the College/University.
- A School Official does not necessarily need to be paid by the College/University.
- For example, if a student needs access to private Educational Data for an official volunteer project, they could be a School Official.

Health Records

Student health records are Educational Data under FERPA/MGDPA.

- Student health records are NOT typically subject to the HIPAA Privacy Rule.
- Only health records maintained by a covered component/operation as defined by HIPAA regulations are subject to the HIPAA Privacy Rule.
- Health records maintained by admissions, the student health center, disability services, and for academic purposes are not subject to the HIPAA Privacy Rule.

Free Application for Federal Student Aid Data

- Data collected on the FAFSA form can only be used in the administration and awarding of federal financial aid.
- Data collected on the FAFSA may also be disclosed to “scholarship granting” organizations with the student’s consent.

Directory Data

“Directory Data” is public data under the MGDPA.

- This is different from the default under FERPA.
- Each campus defines what is directory data. The definitions differ from campus to campus.
- Students can “suppress” directory data upon request. This makes it PRIVATE.
- “Limited Directory Data” can only be disclosed for a particular purpose as defined in policy.

Other Common Exceptions

- Transfer Exception
- Certain Federal or State Programs
- Financial Aid Exception
- Accreditation
- Health or Safety Emergency
- Solomon Amendment
- The Pop Quiz Exception
- Certain F-1, M-1, J-1 Data
- 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 your campus' Data Practices Compliance Official.

Non-FERPA Records

- "Sole-Possession" records:
  - Faculty's notes, not shared with anyone, 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-work study student employees;
- Alumni records created after graduation.
- All of these records are subject to the MGDPA.

Potential Employers

- If a student requests a reference, you should ask them to sign a FERPA consent to send it to the potential employer, or give the student the reference directly.
- If a potential employer asks you about a student, you should ask them to share the student's consent document.
- Career services and other appropriate departments could obtain student consent ahead of time in order to share Educational Data with potential employers.

Parents

- Unlike parents of K-12 students, parents of College/University students do not have a right to inspect FERPA protected data of the student without the student's consent.
- Some campuses allow the "dependent exception."
- Keep in mind that parents, even if authorized, should follow data access procedures.
- Under FERPA, typically only students can access or grant access to their own FERPA protected data.
- PSEO students are College/University students for FERPA purposes.

Guardians and Conservators

- If a student's court appointed guardian/conservator/guardian-ad-litem approaches you for student data, the College/University should ask them for the court order placing them in their position.
- The court order will show the legal powers of the guardian/conservator/guardian-ad-litem.
- A conservator may have the ability to give consent.

Examination Data

- The MGDPA defines Examination Data used to administer exams, including academic exams.
- Examination Data is not public if "the disclosure of which would compromise the objectivity or fairness of the testing or examination process."
  - Data created before an exam, during the exam period, and before you distribute grades are usually private data.
  - Data of old exams may not be private in all circumstances.
- After the examination period has passed, students have a right to inspect examination materials.
  - We don't have to provide copies, but students can take pictures during inspection.

Law Enforcement & Emergency Requests

- A law enforcement agency must have consent or a valid court order or subpoena to obtain Educational Records.
- Third parties, including law enforcement, cannot use subpoenas to obtain other private data.
- FERPA has a health/safety emergency exception. The MDGPA has a similar rule for employee data.
  - The health/safety exception needs to be authorized by administration, it is not an individual decision.
- Please follow your campus' internal process for answering law enforcement data inquiries.

Data Practices Compliance Officials

- Responsible for responding to MGDPA requests, and answering questions about access to public data.
- May have compliance responsibilities as directed by the College/University.
- DPCO's are not required to answer questions about the data itself.
- The Office of General Counsel maintains a list of DPCO's.

Data Breaches

Minn. Stat. 13.055 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.

Data Breaches (2)

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.

IMPORTANT: The Federal Department of Education now requires same-day notification of suspected or actual data breaches.

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

Contact Information

Daniel G. McCabe

Assistant General Counsel

Office of the General Counsel

Daniel.McCabe@minnstate.edu

651-201-1833

MINNESOTA STATE

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

651-201-1800
888-667-2848

www.MinnState.edu