2014 DATA PRACTICES ACT AMENDMENTS - NEWS YOU NEED TO KNOW

Kris Kaplan
Deputy General Counsel

Sarah McGee
Assistant General Counsel

Minnesota State Colleges and Universities

The Minnesota State Colleges and Universities system is an Equal Opportunity employer and educator.
Overview

- Data Handling Laws and Standards
- 2014 MGDPA Amendments
  - Contracts with private companies
  - Security assessments of “personal information”
  - Security safeguards procedures
  - Breach notification and reporting requirements
  - Other miscellaneous amendments
  - Accuracy and completeness challenges
Minnesota Government Data Practices Act
Minnesota Statutes Chapter 13

- Applies to all government data, wherever located
- Presumes data are public – available on request
  - But most personnel and educational data are private – subjects generally have right to access to data about themselves and otherwise control access as permitted by law.
- Government entities must keep data secure and maintain with appropriate privacy protections
  - Administrative
  - Physical
  - Technical
Other Data-Related Laws and Standards

- Family Educational Rights and Privacy Act (FERPA)
- HIPAA (limited applicability to colleges/universities)
- Gramm Leach Bliley (certain business records)
- PCI DSS (industry standards for credit card information)
- Official Records Act, Minn. Stat. §15.17 ("... public officers shall make and preserve all records necessary for full and accurate knowledge of their official activities...")
- Records Management Statute, Minn. Stat. §138.17 (records disposition panel approves retention schedules for official records)
2014 Amendment to Contracting Language
Minn. Stat. §13.05, subd. 11

- In response to Minnesota Supreme Court case, 2014 legislature amended MGDPA to clarify that government contractors are, in fact, subject to the MGDPA.

  - **Privatization.** (a) If a government entity enters into a contract with a private person to perform any of its functions, the government entity shall include in the contract terms that make it clear that all of the data created, collected, received, stored, used, maintained, or disseminated by the private person in performing those functions is subject to the requirements of this chapter and that the private person must comply with those requirements as if it were a government entity. All contracts entered into by a government entity must include a notice that the requirements of this subdivision apply to the contract. Failure to include the notice in the contract does not invalidate the application of this subdivision. The remedies in section 13.08 apply to the private person under this subdivision.

- Contract must include notice language, but requirements apply regardless.
- New language being added to system templates . . .
New System Template Language

**GOVERNMENT DATA PRACTICES ACT.** The requirements of Minnesota Statutes § 13.05, subd. 11 apply to this contract. The CONTRACTOR and MnSCU must comply with the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13, as it applies to all data provided by MnSCU in accordance with this contract, and as it applies to all data, created, collected, received, stored, used, maintained, or disseminated by the CONTRACTOR in accordance with this contract. The civil remedies of Minnesota Statute §13.08 apply to the release of the data referred to in this clause by either the CONTRACTOR or MnSCU.

In the event the CONTRACTOR receives a request to release the data referred to in this clause, the CONTRACTOR must immediately notify MnSCU. MnSCU will give the CONTRACTOR instructions concerning the release of the data to the requesting party before the data is released.
2014 MGDPA Amendments: Annual Security Assessment

- **Comprehensive security assessments** (Minn. Stat. 13.055, subd. 6) now required *at least annually* of any *personal* information defined as:
  - First name or first initial and last name
  - In combination with any one or more of the following if not encrypted or otherwise secured:
    - Social Security Number;
    - Driver’s license number or Minn. ID card number; or
    - Account number or credit card or debit card number in combination with any required security code or password that would permit access to the individual’s financial account.

- Where on campus does such data reside? How is it protected?
2014 MGDPA Amendments: Security

Minn. Stat. §13.05, subd. 5 requires procedures to:

- Assure that all data on individuals is accurate, complete and current;

- Establish appropriate security safeguards for all data on individuals; now expanded to require:
  - Procedures for ensuring that data that are not public are only accessible to persons whose work assignment reasonably requires access to the data and is only being accessed by those persons for purposes described in the procedure; AND
  - Develop a policy incorporating these procedures, which may include a model policy governing data sharing with other government entities as authorized by law.
Compliance with New Security Procedures Requirements

- Review technical data access controls;
- Review and document work assignment access needs;
  - Consider adding description of authorized data access to position descriptions;
- Training, training, training!
- Updated system guidance to come.
2014 MGDPA Amendments: Breach

- **Breach in Security** definitions amended (underlined):
  - A “breach” means *unauthorized acquisition* of data maintained by a government entity (*including a contractor*) that compromises the security and classification of the data.
  - “Good faith acquisition” of *or access* by an employee, contractor, or agent is not a breach if:
    - the government data is not provided to *or viewable by an unauthorized person*; or
    - accessed for a non-work purpose, under established procedures.
Breach Definitions Amended: Breach

- *Unauthorized acquisition* means obtaining, accessing or viewing data without informed consent and with the intent to use the data for nongovernmental purposes.

- *Unauthorized person* means access without a work assignment that reasonably requires access or regardless of work assignment, for a purpose not described in the new security procedures.

  - Thus, an employee may be an unauthorized person if accessing data for improper purpose even if generally authorized to access the same data for work assignment.
2014 MGDPA Amendments: Breach

- **Breach Notification and Investigation Report** Minn. Stat. §13.055, now requires *written notice* to individual subject of breach informing him/her:
  - that a report will be prepared;
  - how to obtain access to the report; and
  - that he/she may request a copy to be delivered by mail or e-mail.

- Upon completion of investigation and final disposition of employee discipline (if any) a report shall be prepared on the facts and results. (This is in addition to any report required to the OLA of any “improper use of not public data.”)
Breach Report Requirements

- If breach involves unauthorized access to or acquisition of data by an employee, **contractor**, or agent, the report must at a minimum include:
  - A description of the type of data that were accessed or acquired;
  - The number of individuals whose data was improperly accessed or acquired;
  - Names of employees responsible for the unauthorized access or acquisition *if* there has been a final disposition of discipline;
  - The final disposition of any disciplinary action against each employee, *if* any.
System Breach Guideline

- Current guideline 5.23.1.13 under review
- Please contact OGC for assistance in determining breach notification obligations.
2014 MGDPA Amendments: Penalties

- Penalties section, Minn. Stat. §13.09, amended to state that any individual whose conduct constitutes the knowing unauthorized acquisition is guilty of a misdemeanor;
  - And may be just cause for discipline or termination of an employee.
2014 MGDPA Amendments: Miscellaneous

- *Safe at Home* data, Minn. Stat. §13.045, requires government entities to honor privacy of program participants including identity or location data.

- Checking Account Numbers, Minn. Stat. §13.37, subd. 1 (a), are now specifically classified as *security information*. 
Accuracy or Completeness Challenges

Individuals may challenge accuracy/completeness of their data; Minn. Stat. §13.04, subd. 4

- Data “in dispute” must include subject’s statement of disagreement if disclosed;
- Appeal to Department of Administration – if not resolved, to OAH for Contested Case hearing under Ch. 14

Minn. S. Ct. recently decided that employees may use this process to challenge performance evaluations. *Schwanke v. Department of Admin*, 851 NW2d 591 (Minn. 2014).
Impact of *Schwanke* Decision?

- Court’s decision focused on alleged factual inaccuracies, but difficult to draw fact/opinion line.
- Apply to students? Probably, but FERPA also has procedure for challenging “inaccurate or misleading” records.
  - Grade challenges?
- Sample MGDPA procedure in Data Practices Toolbox [www.ogc.mnscu.edu](http://www.ogc.mnscu.edu)
- Legislature expected to take up issue in 2015.
Contact Information
Minnesota State Colleges & Universities
System Office

- Kris Kaplan, Deputy General Counsel
  kristine.kaplan@so.mnscu.edu
  (651) 201-1749

- Sarah McGee, Assistant General Counsel
  sarah.mcgee@so.mnscu.edu
  (651) 201-1410

Office of General Counsel
www.ogc.mnscu.edu

Please take a few minutes to complete our poll!