FYi

From the Information Policy Analysis Division

Volume 13 Issue 3
Summer 2014

New Sample Policy Guidance

The 2014 legislative session was a big one for data practices! While a summary of all the data practices related changes appeared in our last newsletter, we want to specifically draw attention to the changes in Minnesota Statutes, section 13.05, subd. 5.

In response to the heightened concern regarding unauthorized access to not public data, the Legislature created an additional duty for a government entity's data practices Responsible Authority: to establish procedures that ensure not public data are only accessible to persons whose work assignment requires access to the data, as well as develop a policy incorporating those procedures. The new legislation reads (in *italics*):

> Subd. 5. Data protection. (a) The responsible authority shall:
> (2) establish appropriate security safeguards for all records containing data on individuals, *including 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*
> *(3) develop a policy incorporating these procedures, which may include a model policy governing access to the data if sharing of the data with other government entities is authorized by law.*

There are several ways government entities can meet these legislative duties. Our agency chose to update an already existing document, its Inventory of Not Public Data (required in section 13.025, subd. 1), by creating a new section that documents which employees have access to specific not public data maintained by Admin.

Further, Admin adopted the Policy for Ensuring the Security of Not Public Data, which limits access to not public data to the employees who need the data for their work assignments, the responsible authority and data practices compliance official, as necessary, and entities authorized by law.

In addition, entities can also update employee position descriptions with language authorizing the employee to access not public data for work purposes, or develop approval forms that document access to not public data that is acknowledged by both the supervisor and the employee to fulfil duties under the new legislation.

As always, IPAD is here to help. We can provide assistance through our policy guidance, or you can feel free to contact us with questions you have while developing your own policies and procedures. We'd also appreciate any feedback on the policy guidance and any ideas you have about compliance.

Inside this issue:

Information Policy Analysis Division

Admin Minnesota
DEPARTMENT OF ADMINISTRATION

Case Law Update

In ***Schwanke v. Minnesota Department of Administration,*** File No. A12-2062 (Minn. Aug. 6, 2014), the Minnesota Supreme Court affirmed the Court of Appeals decision that a public employee can challenge a performance evaluation as inaccurate or incomplete government data under the data challenge appeals process in Minnesota Statutes, section 13.04, subd. 4. The Department originally declined to accept the challenge appeal, as a performance evaluation contains subjective impressions, but the court held that the Commissioner does not have the authority to dismiss appeals that are not resolved informally without first issuing a notice and order for a contested case hearing at the Office of Administrative Hearings.

In ***Minnesota Joint Underwriting Association v. Star Tribune Media Company***, File No. A13-2112 (Minn. Ct. App. Jun. 9, 2014), the Minnesota Court of Appeals reversed the district court's decision and found that the Minnesota Joint Underwriting Association (MJUA) is not a government entity for the purposes of the Data Practices Act. The court held that the enacting statute is ambiguous, and in comparing other enacting statutes to the MJUA's, the court determined that if the Legislature wanted to make the MJUA subject to the Act, it would have included that provision in the enacting statute.

In ***Mooers v. City of Lake City, et. al***, File No. A13-2197 (Minn. Ct. App. Jul. 7, 2014, unpublished), a city council closed a meeting to discuss an anonymous complainant's allegations and decided, in an open meeting, that the allegations were unfounded. The local newspaper subsequently printed an article discussing the complaints and the plaintiff brought a claim against the city for, among others, invasion of privacy and data practices violations. The court dismissed all claims determining in part that the publication of private facts was of legitimate concern to the public and the plaintiff failed to point to an actual record or person that disseminated private data.

The following federal district court summaries relate to data breaches of private data in the state Driver and Vehicle Services (DVS) database under the federal Driver's Privacy Protection Act (DPPA).

In ***Ray v. Anoka County, et al.***, File No. 14-539 PAM/TNL (D. Minn. 2014), the court dismissed all DPPA claims based on the four-year statute of limitations and because the plaintiff failed to plead objective facts demonstrating that the access was for impermissible purposes.

In ***Kampschroer v. Anoka County, et. al.,*** File No. 13-cv-2512 SRN/TNL (D. Minn. 2014), the court, while holding that a four-year statute of limitations applies to DPPA violations, refused to dismiss any claims involving lookups after 2004 because plaintiffs sought assurances by the Department of Public Safety on numerous occasions, beginning in 2008, and were assured each time that their information was secure. The court also refused to dismiss the DPPA claims against the government defendants because the pattern of the lookups indicated that many were not for law enforcement purposes.

Continued on page 4.

Advisory Opinion Update

Open Meeting Law; Summary of Conclusions

Opinion 14-007: A member of the public asked whether a City had complied with Minnesota Statutes, section 13D.05, subd. 3(a), regarding a summary of the conclusions of an employee's performance evaluation at the next open meeting. The City did not comply when it failed to provide a summary at the next open meeting and because the statement provided at a subsequent meeting was insufficient.

Applicants for Appointment

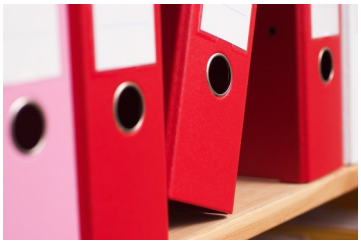
Opinion 14-008: A School District planned to fill an open seat on its school board by appointment. The media asked for public data about the applicants under Minnesota Statutes, section 13.601. The District first responded that the data were private under Minnesota Statutes, section 13.43, but gave the data to the media six days after the application period ended, after the school board approved a resolution that it no longer considered board members to be employees. The District's initial response was incorrect, but because the District was obligated to redact private applicant data per section 13.601, the District's eventual response was prompt and reasonable.

Education Data

Opinion 14-009: An educational entity asked whether it could designate limited directory information as described in the federal Family Educational Rights and Privacy Act's (FERPA) regulations consistent with Chapter 13. Educational entities can designate limited directory information and the federal government affords greater privacy protection to limited directory information such that access could be restricted to specific parties, for specific purposes, or both.

Open Meeting Law; Printed Materials

Opinion 14-010: A member of the public asked about the copy of printed materials at a township meeting. Minnesota Statutes, section 13D.01, subd. 6, requires public bodies to make at least one copy of any printed materials distributed to the public body members available during a public meeting. The member of the public stated that the Township Planning Commission did not include a copy of the draft comprehensive plan. The Township's attorney responded that the Commission did include the comprehensive plan in the public packet of materials. Though the Commissioner could not resolve the factual dispute, he offered some practical advice to the Township, including offering more than one copy of the materials, posting the materials online, or listing the contents of the materials.



Data Requests: Public or Private?

When a person requests **public data** and provides identifying information, then the request and identity are public data**.** The Commissioner of Administration recently opined in Advisory Opinion 14-006 that, because Chapter 13 does not classify data related to public data requesters, "those data are presumptively public."

If an individual requests **private data**, then his/her identity as a data requester is **private** because the underlying data are private. For example, an entity cannot release the identity of a requester and information about the request if an individual requests data relating to his/her public assistance benefits because the data are private.

While there is no requirement in the Data Practices Act to notify requesters that their request is public, IPAD recommends including a note in the entity's Policy for Public Requesters that the data are public and that, in the alternative, a requester can make an anonymous request. Even if the requester is anonymous, the request itself remains public.

Case Law, cont.

In ***Heglund v. Aitkin County, et al.,*** File No 14-296 ADM/LIB (D. Minn. 2014), the court dismissed the DPPA claims older than four years under the statute of limitations, but refused to dismiss all claims against the government as the plaintiffs had pleaded a plausible claim. The majority of lookups had come from one of the plaintiff's previous workplaces, the information was looked up within seconds of each plaintiff, and the lookups were by name rather than license plate number. The court ruled that this evidence was sufficient to withstand a motion for summary judgment. In accord with other federal district court cases, the court dismissed the plaintiffs' invasion of privacy claim because there is no reasonable expectation of privacy in driver's license data.

In ***Shambour v. Carver County, et. al,*** File No. 14-566 RHK/LIB (D. Minn. 2014), the plaintiff alleged her driver's license information had been impermissibly accessed by numerous government entities on the basis that her information had been looked up over 50 times, she was well known to law enforcement, she had never been under investigation, and her information had been looked up at odd hours of the night. The court dismissed all claims older than four years under the statute of limitation, as well as the claims against the officials who were responsible for maintaining the database. The court refused to dismiss the claims against the individual defendants, however, because the plaintiff had pleaded facts sufficient to allege her data was impermissibly accessed. The invasion of privacy claim was dismissed in accord with the other federal district court cases.

Office of Administrative Hearings

The following summaries from the Office of Administrative Hearings relate either to general data practices issues, or were a result of the expedited administrative remedy process in Minnesota Statutes, section 13.085.

In the Matter of Minnesota Department of Natural Resources Special Permit No. 16868 (December 12, 2012) Issued to Lynn Rogers (84-2001-30915)

In February 2014, the Department of Natural Resources (DNR) requested a protective order to classify Dr. Rogers' research data as confidential to obtain that data through discovery. The classification was granted and Dr. Rogers produced the requested research. The DNR then requested removal of the confidential classification because it was not trade secret or proprietary data.

The Chief Administrative Law Judge found that researchers may acquire a proprietary interest in their research in appropriate circumstances. The DNR failed to establish any public purpose for why it should not protect the research. The motion to terminate the protective order was denied.

In the Matter of North Dakota Pipeline Company (80-0305-31410)

North Dakota Pipeline Company (NDPC) was required to provide the Minnesota Public Utilities Commission (MPUC) with a list of all affected parties in its planned pipeline construction. NDPC requested that MPUC not disclose the list because it was trade secret data. MPUC declined that request, and NDPC filed a complaint with the Office of Administrative Hearings that MPUC violated the Data Practices Act in designating trade secret data as public.

The Administrative Law Judge found that the pipeline's path is public record and anyone could use tax rolls and mailing addresses to compile it. The fact that NDPC included more information on the list than required, and spent extra time and money to do so, does not prevent MPUC from disclosing the data. The complaint against MPUC was dismissed.