



Data Practices 101

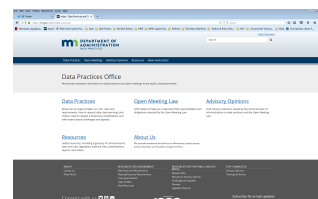
Fire Chiefs Annual Conference

Taya Moxley-Goldsmith
Data Practices Office

1

We are a statewide resource

- Data Practices Office (formerly IPAD)
 - Informal advice/technical assistance
 - Commissioner of Administration advisory opinions
 - Website and informational materials:
<https://mn.gov/admin/data-practices/>
 - Listserv and newsletters
 - Legislative assistance
 - Training



2

Topics

- Overview of data practices requirements
- Remedies and penalties
- Law enforcement data
- Medical data
- Personnel data

3

Data Practices Overview

4

Government data practices & official records

- **MN Government Data Practices Act, Ch. 13**

- Presumes government data are public
- Classifies data that are not public
- Access rights for the public and data subjects
- Data on individuals are accurate, complete, current, and secure

- **Official Records Act** requires preservation of all records necessary to a full and accurate knowledge of official activities

- **Records Management Statute** requires records retention schedules approved by records disposition panel

- MN State Archives: www.mnhs.org/preserve/records/gov_services.htm

5

Lifecycle of government data

Government Data Practices Act
Administer Data



Official Records Act
Create and Maintain Data



Records Management Statute
Destroy data



6

Government data defined

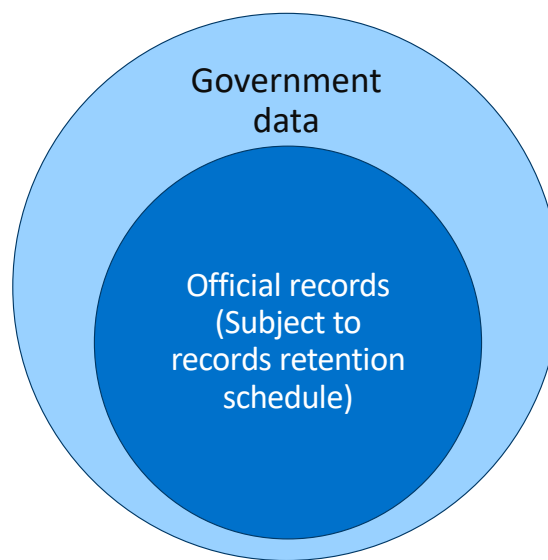
“All data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use.”

(Minn. Stat. § 13.02, subd. 7)



7

Official records vs. government data



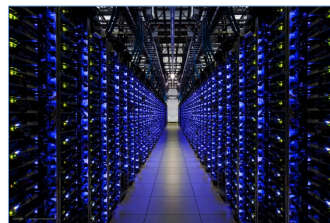
8

Maintaining government data

Government is not required to maintain data in particular formats or systems of organization

However...

Data must be “easily accessible for convenient use.”



9

What do you think?

- 1) Is the email government data?
- 2) Is the email an official record?
- 3) Can you destroy/delete the email?

- An email to your coworker asking if they will print a copy of the agenda for a staff meeting
 - Government data
 - Not official record
 - Delete at any time
- An email formally complaining about a fire department employee
 - Government data
 - Probably an official record
 - If an official record, retain according to retention schedule
- An email to your mom wishing her a happy birthday
 - Possibly “personal” data and not government data
 - Not an official record
 - Delete at any time



10

Classification of government data

Data on individuals	Data not on individuals
Data that identify someone <ul style="list-style-type: none"> Public employee's telephone number Name and address of adult arrestee Athlete of the week photograph 	Data that do not identify someone <ul style="list-style-type: none"> Makes and models of fleet trucks Names of companies that are preferred vendors List of government websites

11

Classification of government data

Classification	Meaning of classification	Examples
Public	Available to anyone for any reason	Employee name & salary
Private/ Nonpublic	Available to: <ul style="list-style-type: none"> Data subject Those in the entity whose work assignment requires access Entities authorized by law Those authorized by data subject 	Identity of a caller in a mental health emergency
Confidential /Protected nonpublic	Available to: <ul style="list-style-type: none"> Those in the entity whose work assignment requires access Entities authorized by law Not available to the data subject	Active criminal investigative data

12

Response time

	Member of the Public (Section 13.03, subd. 3; Minn. Rules, part 1205.0300)	Data Subject (Section 13.04, subd. 3)
Inspection and/or copies	Appropriate and prompt, a reasonable amount of time	Immediately, if possible or 10 business days

13

Charging for government data

	Member of the Public	Data Subject
Inspection	No charge or fee allowed	No charge or fee allowed
Copies	<ul style="list-style-type: none"> ❖ 25¢ per page 100 or fewer, black and white, legal/letter size paper copies ❖ Actual cost <ul style="list-style-type: none"> ◆ All other copies ◆ Time for search and retrieval ◆ Time to make and transmit ◆ Materials ◆ No charge to separate public from not public data ◆ Electronic data 	<ul style="list-style-type: none"> ❖ Actual cost <ul style="list-style-type: none"> ◆ Time to make and transmit ◆ Materials ◆ No charge for search and retrieval ◆ No charge to separate public from not public data ◆ No charge to redact private or confidential data about others

14

Required policies/procedures

- Access Policies
 - Policy for the Public (section 13.025, subd. 2)
 - Policy for Data Subjects (section 13.025, subd. 3)
- Data inventory (section 13.025, subd. 1)
- Policy for Ensuring the Security of Not Public Data (Section 13.05)
- Model policies:
<https://mn.gov/admin/data-practices/data/rules/policies/>

15

Best practices in handling data requests

- Create and update your required policies and procedures
- Consider entity structure
 - RA & DPCO
 - Designees?
- Requests in writing
- Document charges for copies



16

Responding to: public data requesters

- Clarify if not clear
- Data do not exist
- Data exist and are public
- Data are not public
 - Must give statutory basis for denying access
- If asked, must explain meaning of data
- Not required to create data or answer questions
- Cannot ask requesters to ID themselves or say why they want data

17

Responding to: data subjects

- Clarify if not clear
- Data do not exist
- Data exist and are about the requester
 - Verify identity
 - Six-month “exception”
- Data are confidential or private about someone else, or otherwise not public
 - Must give statutory basis for denying access
- If asked, must explain data

18

Tennessee warning notice and informed consent

- Tennessee Warning
 - At collection
 - Private/confidential data *from* data subject *about* subject
 - Includes: Purpose/use, whether subject can refuse, consequences, and entities data can be shared with
- Informed consent
 - After collection
 - In writing
 - Not coerced
 - Identify consequences



19



Data breaches

Minn. Stat. §13.055

- “Breach of the security of the data”
 - Unauthorized acquisition/unauthorized person
 - Access to private or confidential data with
 - **Intent** to use data for nongovernmental purposes
- Requires investigation and public report
- Annual security assessment for “personal information” (See section 235E.61)

20

Data breach, cont.

Breach Examples	Corrective Action	13.055 Notice
Accidentally accesses not public database	Yes	No
Incorrectly types email address and sends not public data to wrong government employee	Yes	No
Inadvertently reads report with not public data without appropriate work assignment	Yes	No
Looks up driver's license data about new neighbor without appropriate work assignment	Yes	Yes

21

Penalties and remedies

- Remedies (Minn. Stat. §13.08)
 - Action for damages, costs, and attorneys fees
 - Action to compel compliance
- Administrative remedy (Minn. Stat. §13.085)
 - Administrative hearing within 2 years of alleged violation
 - Action to compel compliance
- Penalties (Minn. Stat. §13.09)
 - Willful violation or knowing unauthorized acquisition of not public data = misdemeanor
 - Dismissal or suspension
- Advisory opinions (Minn. Stat. §13.072)

22



DEPARTMENT OF
ADMINISTRATION

Adult Law Enforcement Data

Minnesota Statutes, Section 13.82

23

Application

- Applies to agencies which carry on a law enforcement function
- Includes:
 - Municipal police and county sheriff departments
 - Fire departments
 - BCA, state patrol, POST
- Does not include prosecuting attorneys
 - Informal AG opinion disagrees with advisory opinion 01-079
 - Public prosecutors in original provision; removed in 1981 amendment
 - Section 13.393 applies to data held by government attorneys
 - Local prosecution authorities are criminal justice agencies

24

What's public?

Is there an active investigation?

- Yes
 - The following data are **public**, subject to protection of certain identities:
 - Arrest data
 - Request for service data
 - Response or incident data
 - Criminal investigative data presented in court
- No
 - All inactive investigation data are public (subject to several exceptions)

25

Request for service data

Requests by the public for law enforcement services ***shall be public***:

- Nature of the request or the activity
- Name and address of the individual making the request (unless protected identity)
- Time and date of the request or complaint
- Response initiated and the response or incident report number

26

Response or incident data

Data describing the agency's response to a request for service, or actions taken by the agency on its own initiative ***shall be public***:

- Date, time and place of the action
- Agencies, etc. participating in the action (unless protected identities)
- Any resistance encountered, pursuit engaged in, or weapons used
- Brief factual reconstruction of events associated with the action
- Names and addresses of witnesses to agency action or incident (unless protected identities)

27

Response or incident data, cont.

- Names and addresses of any victims (unless protected identities)
- Name and location of the health care facility to which victims were taken
- Response or incident report number
- Use of body camera to document the agency's response
- Specific to **traffic accidents**:
 - Dates of birth of the parties involved
 - Whether the parties involved were wearing seat belts
 - Alcohol concentration of each driver

28

Criminal investigations

Active investigative data - data collected or created by law enforcement to prepare a case against a person are **confidential/protected nonpublic**

- Except:
 - Arrest, request for service, response or incident data (public)
 - Protected identities (private)
 - Public benefit data (discretion to release)
 - Exchange of information by law enforcement agencies – “pertinent and necessary” to an investigation
 - Prosecutor shall release to victim upon written request
 - Data presented as evidence in court

29

Inactive investigative data

Inactive investigative data are **public**, except:

- Jeopardize ongoing investigation (confidential/protected nonpublic)
- Reveal protected identities (private)
- Images and recordings (photographs, video, audio records) offensive to common sensibilities (private)
- Certain child or vulnerable adult abuse data (private)
- Certain body camera data (private)

30

When are investigations inactive?

- Decision not to prosecute
- Time to charge expires
- All rights to appeal exhausted or expired
- Not guilty/Exonerated*

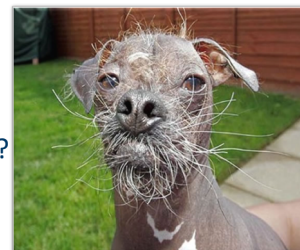


31

Chapter 13 Check!

A member of the press requests a copy of a photo of Jeter, the famously ugly dog, from your agency. The photo is related to a case that was never investigated.

- Can he have it?
 - Yes! Presumptively public.
- What if the photo is part of an active investigation?
 - No. Not “super public” under subd. 2, 3, or 6.
- What about when the case becomes inactive?
 - Yes! Becomes public under subd. 7.



32

Protecting identities

Section 13.82, subdivision 17

Law enforcement **must** protect identities of some individuals

- Undercover law enforcement officer
- Victim or alleged victim of criminal sexual conduct or sex trafficking
- Deceased person unlawfully removed from a cemetery
- Mandated reporter
- Person making a 911 call or name and phone number of service subscriber if either:
 - Reason is for help in a mental health emergency; or
 - Determine would threaten safety of person or property

33

Protecting identities, cont.

Law enforcement **may** protect other individuals, but must make certain decisions:

- Paid or unpaid informant
- Victim or adult witness to a crime
- Juvenile witness



34

911 Calls

Section 13.82, subd. 4

- Recording of 911 call
 - Private data on the caller
- Transcript of 911 call
 - Public
 - Unless it reveals a protected ID under subd. 17
 - Person requesting transcript shall pay actual cost of transcription



35

Other not public law enforcement data

- Child abuse data (private) – subds. 8 and 9
- Vulnerable adult data (private) – subds. 10 and 11
- Certain property data (private/nonpublic) – subd. 20
- Certain pawnshop data (private) – subd. 27
- Financial account or transaction numbers (private/nonpublic) – subd. 30

36



Additional Data Practices Provisions and Topics

37

Fire department video and photos

- Currently, section 13.825 – Body camera data – does **not** apply to firefighters/fire departments
- Video is classified pursuant to 13.82
- All departments should have a policy on taking images while on duty
 - Policy should include the dissemination of those images, including on social media.
 - Consider how to obtain data after collection on personal devices

38

Property complaint data

Minn. Stat. §13.44, subd. 1

- Identities of individuals making complaints about the use of real property
 - Violations of state law or local ordinance
 - Confidential
- What constitutes “use of real property”
 - Weeds in a neighbor’s yard?
 - Loud party next door?
 - Barking dog across the street?



39

Security information

Minn. Stat. §13.37, subd. 1(a)

- Likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury
- Private/nonpublic
 - RA can provide if access will aid public health, promote public safety, or assist law enforcement
- Not a blanket classification – case by case determination
 - RA must explain upon request



40

Medical information

- **HIPAA:** complete an internal legal analysis to determine if meets the definition of “covered entity”
 - Generally, LEAs are not subject to HIPAA privacy rule
 - Possible covered entities: EMT services, group health plans
 - DPO’s HIPAA guidance for government entities:
<https://mn.gov/admin/data-practices/data/types/patient/hipaa/>
- **Minnesota Health Records Act** (Minn. Stat. §144.293, subd. 2)
 - Health records received *directly from a provider* may not be disclosed without consent/specific authority
 - Health information recorded or collected *by law enforcement* is presumptively public (i.e., not “medical records”)
 - EMS/EMTs not “providers” under state law

41





Personnel data

Minnesota Statutes, section 13.43

42

Personnel data – defined Section 13.43

- Government data *on individuals* maintained because an individual is or was an employee of a government entity, applicant for employment, volunteer, or independent contractor
- Reverses general public presumption
 - All personnel data are private except data specifically classified as public.
 - Examples of private data:
 - Performance reviews
 - Supervisor notes
 - Medical documentation

43

Personnel data – public

- **Name**; employee ID; actual gross **salary**; salary range; **terms and conditions of employment relationship**; contract fees; actual gross **pension**; the value and nature of employer paid **fringe benefits**; and the basis for and the amount of any added **remuneration**, including expense reimbursement
- Job title and bargaining unit; job description; **education and training background**; and previous work experience
- Date of first and last employment
- **Existence and status of any complaints or charges** against the employee, regardless of whether the complaint or charge resulted in a disciplinary action

44

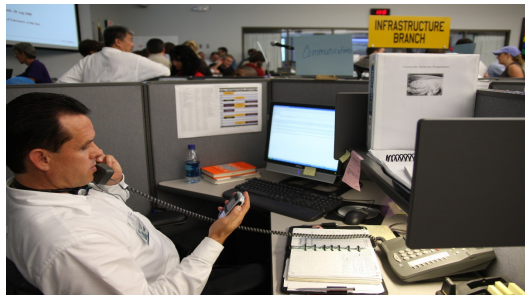
Personnel data – public, cont.

- **Final disposition of any disciplinary action** together with the **specific reasons** for the action and **data documenting the basis** of the action
- **Complete terms of any agreement settling any dispute** arising out of an employment relationship, including a buyout agreement; except that the agreement must include **specific reasons** for the agreement if it involves the payment of more than **\$10,000 of public money**
- Work location; a work telephone number; badge number; **work-related continuing education**; and honors and awards received
- **Payroll time sheets** or other comparable data that are only used to account for employee's work time for payroll purposes, except to the extent that release of time sheet data would reveal the employee's reasons for the use of sick or other medical leave or other not public data

45

What do you think?

- Government employees create and maintain various data as a part of their official tasks and duties.
 - Are all of the data that an employee creates or maintains personnel data?



46

Not everything is personnel data

- Employee must be the individual subject of the data
- Consider:
 - Meeting notes
 - Reports
 - Correspondence about an official activity
- Some “personal” data

47

Personal data

- How are emails and voicemail messages on an employee’s personal matters classified?
 - Government data?
 - Policy for incidental use of government equipment?

48

Legislative issues

- Joint Committee on Data Practices
- Ones to watch
 - Data breaches
 - Legislature subject
 - Drones



49



Questions?

Data Practices Office

651-296-6733

info.ipad@state.mn.us

<https://mn.gov/admin/data-practices/>

Twitter: @mngovdata

YouTube training videos: user/infoipad

50