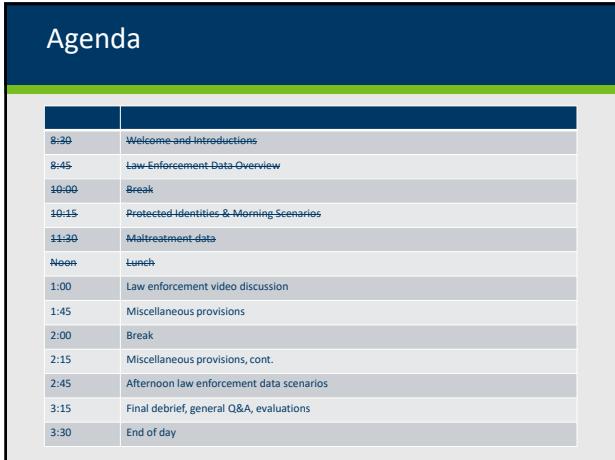




1



2



3

Body-worn camera (BWC) data

§ 13.825 (202)

- Most inactive BWC video data = private/nonpublic
- Active investigative data are confidential/protected nonpublic
- BWC data are public if there is:
 - Discharge of firearm in the course of duty
 - Incident results in substantial bodily harm
 - Data subject makes data public, with applicable redactions
 - Public employee disciplinary data
 - Individual dies as a result of officer's use of force; public within 14 days after incident*

4

BWC data access, generally

- Data subjects include:
 - Anyone who can be seen or heard
 - Peace officer who collects the data
 - Peace officers who can be seen or heard
- Access by data subjects:
 - Data subject can access (inspect) unredacted video
 - Copies must be redacted, unless consent from other data subjects
 - On duty officers who are not undercover may not be redacted
- Access to data with no identifiable individuals:
 - Nonpublic data – need to determine subject of data, if any

5

BWC data access – deadly use of force

13.825, subd. 2(b)-(d)

Deadly use of force incident, a law enforcement agency must:

- Allow next of kin, their lawyer, and other parent of deceased's children to inspect data within five days of request
 - Agency may deny access if there is a compelling reason why inspection would interfere with active investigation
 - Must provide prompt, written denial as well as inform family that relief may be sought from district court per section 13.82, subd. 7
- Videos are classified as public (with applicable redactions) within 14 days after incident
 - Agency may withhold access if it asserts disclosure would interfere with active investigation, in which case it is classified by 13.82, subd. 7

6

BWC data access – state accident reports
13.825, subd. 4(c)

- A person entitled to State crash report under §169.09
- Copies of unredacted data from *all* body cams used in investigation, including data on others and active investigative data.
- May provide redacted video if:
 - compelling reason that access to the data would interfere with an active investigation;
 - the data are clearly offensive to common sensibilities; or
 - the data are classified as not public by other provisions under Ch. 13.

7

Unmanned Aerial Vehicle (UAV) data (drones)
Minn. Stat. §626.19

- Generally private/nonpublic
- Active criminal investigative UAV data = confidential/protected nonpublic.
- Inactive criminal investigative = public
- Other not public data retain classification
- Can be disclosed as necessary in emergency situations as described in statute
- If no investigation, must be deleted within 7 days



8

Steps in determining access to videos

- What kind of video is it?
- Is there an active investigation?
- What section classifies the data?
- What is the classification?
- Who can view the unredacted video?
- Who can have a copy?
- Does public benefit data apply?

9

What type of video is it?

- Body camera video – § 13.825
- Drone data/video – § 626.19
- Other video: Squad video, cellphone video, taser camera, gun camera, etc. – § 13.82 or presumptively public

10

Is there an active investigation? Yes

Dash cam video

- § 13.82
- Confidential/protected nonpublic
- Those within entity and with statutory authority
- No obligation to provide access to data requesters
- Consider public benefit

Body camera video

- §§ 13.825/13.82
- Confidential/protected nonpublic
- Those within entity and with statutory authority
- No obligation to provide access to data requesters, generally
- Consider public benefit

11

Is there an active investigation? No

Dash cam video

- Classified by § 13.82
- Inactive investigative data = public
- Exceptions: protected IDs

Body camera video

- Classified by § 13.825
- Private data on individuals in video
 - Exception: Data presented as evidence in court are public under 13.82, subd.7
- Data subjects can view unredacted – where they are seen or heard
- Data subject can have copy with other data subjects redacted
 - On duty officers cannot be redacted
- Data subject can ask video be made public
- Undercover officers must be redacted

12

What do you think?

An individual who can be seen and heard in a body camera video (a data subject) asks to view the video. The video is inactive investigative data and not introduced as evidence in court. The individual can be seen talking to peace officers for 8 minutes of 1 hour video.

Can the requester access the full hour?



13

What do you think - Answer

- No.
- The requester may only have access to the portion of the video where they can be seen and/or heard
- The requester can view/inspect their portion unredacted (except undercover officers)
- If the requester wants a *copy* of the 8 minutes, any non-officers must be redacted unless they have given consent.

14

What do you think?

A member of the public asks for access to a body camera video from an inactive case. The video was not used as evidence in court.

They also ask for inactive dash camera video.

What can the requester have access to?



15

What do you think - Answer

- Most inactive body camera video = private subject to specific exceptions (§ 13.825)
- Most inactive dash camera video = public (§ 13.82)
- Unless it is offensive to common sensibilities, entity determines = private
- Child or vulnerable adult maltreatment videos where the case did not go through a court process.

16

What do you think?

On Monday, Officers Diaz and Scully respond to a domestic call and activate their body-worn cameras. The officers enter the home and observe a man hitting a woman. A child and another adult woman are in the same room. The officers arrest the man and talk to the others.

Neighbor Fred Rogers requests the BWC video on Tuesday. Can he have it?



17

What do you think - Answer

- The individual was arrested – there are active investigative data.
- The data in the video are confidential/protected nonpublic – Mr. Rogers cannot have the video.
- What happens when the case becomes inactive?
 - No prosecution = private, folks who can be seen or heard can have access
 - Prosecution:
 - Video presented as evidence in court = public
 - Video not presented as evidence in court, inactive = private

18

What data practices issues do you see when working with body camera data or other law enforcement videos?

19



Miscellaneous Law Enforcement Data

20

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?

21

What do you think?

Question: A requester asks for all police reports about his apartment for the last year. Most of the calls are noise complaints by a neighbor. What should you release?



22

What do you think - Answer

Answer: The reports will likely contain both public and not public data. Most data in police reports are public under §13.82 or the general presumption.

However, §13.44 classifies a complainant's ID as **confidential** when:

- Complaint is about violations of state laws or local ordinances AND
- Concern the use of *real* property

23

Traffic accidents

State Accident Report, Minn. Stat. §169.09, subd. 13 (203)

- Reports are not public but DPS or any LEA shall release upon written request to:
 - Parties involved
 - Others suffering injury to person or property
 - Representatives of the estate or surviving spouse
 - Legal counsel and insurers for above
- Must redact identifying info on juvenile who:
 - Was taken into custody, or
 - Suspected of a "major traffic offense" (§ 260B.225)
- Charging for copies
 - DPS can charge \$5
 - LEA charge per Ch. 13

24

Traffic accidents - public law enforcement data

- Local law enforcement traffic accident data are classified under section 13.82
- If no local report, LEA must provide access to §13.82, subd. 3 or 6 in redacted State Accident Report.



25

Driver's license data

- Federal law: Driver's Privacy Protection Act (DPPA), 18 USC §§2721-2725

- State DMV employee or contractor shall not knowingly disclose information in motor vehicle records
- Certain permissible uses

- Minnesota law:

- Minn. Stat. §171.12, subd. 7
 - Data used to obtain a driver's license must be treated as provided in the DPPA
- Minn. Stat. §171.07, subd. 1a (DVS photographs) – private, but do not have to be provided to the subject



26

What do you think?

How are vehicle identification numbers classified?



27

What do you think - Answer

Presumptively public. But consider:

- § 13.82, subd. 7 may be applicable if there is an active investigation.
- § 13.82, subd. 20 classifies data that uniquely describe lost, stolen, confiscated or recovered property as private/nonpublic.
- § 13.37 – case-by-case basis (AO 13-010)

28



15-minute break

29

Data on Decedents

Minn. Stat. §13.10

Not public data about data subjects who have died

- Private data become private data on decedents
- Confidential data become confidential data on decedents

Representative of decedent exercises access rights

- Personal representative of decedent during administration period
- If none, then surviving spouse or any child of decedent
- If no spouse or children, then parents of the decedent

Data become public when:

- 10 years have elapsed since death or presumed death; *and*
- 30 years have elapsed since creation of data

30

Automated License Plate Reader Data (ALPR)

Minn. Stat. § 13.824

- ALPR data are private/nonpublic
 - “Non-hit” data cannot be retained more than 60 days
 - Independent, biennial audits required
 - Audit guidance: https://mn.gov/admin/assets/ALPRaudit_tcm36-307907.pdf
 - Must send audit results to Commissioner of Administration and designated legislative committees
 - Limits on ALPR data sharing among LE
- Public data:
 - Public log of ALPR use
 - Whether an ALPR was used in arrest
 - Existence of recording technology is public
- ALPR procedures required



31

Criminal background checks

- Examples required by law
 - Law enforcement officers (Minn. Stat. §626.87)
 - School employees, coaches, volunteers (Minn. Stat. §123B.03)
 - Human services licensees (Minn. Stat. Ch. 245C)
- Private data (data subject has access)
- What should LE provide in response to a request?
 - Only public data, or private with consent
 - No active criminal investigative data
 - Body camera data? Probably not
 - Juvenile delinquency data are private and accessible via consent

32

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

33

What do you think?

During an investigation, police officers photograph the contents of an individual's medicine cabinet. Ultimately, the prosecutor declines to pursue the case and the photographs become inactive criminal investigative data.

How are the photos classified?



34

What do you think - Answer

- The photos are classified as **public**
- Data are inactive investigative data under 13.82, subd. 7.
- PD is not a covered entity for purposes of HIPAA.
- The photos are not health records under Minnesota law (not received directly from a health care provider).

35

Domestic abuse data

Minn. Stat. § 13.80

- Data collected pursuant to the Domestic Abuse Act = confidential
 - Once a temporary court order is executed or served – data classified by section 13.82
- Must provide **public** data and certain reports to victim, victim's attorney, or an organization designated by the OJP *for free*.
- Victims can also access **active** investigative data upon written request to the prosecutor (section 13.82, subd. 13)

36

Personnel data in law enforcement agencies

Minn. Stat. §§ 13.43, 626.8457

- LEAs are also employers
- Data maintained as IA/personnel data classified by § 13.43
- The same data might also be maintained as law enforcement data under § 13.82
- Arrest, request for service, and response or incident data regarding agency staff are always public
 - No exception even if used in personnel/internal affairs investigation
 - Can never be withheld as private personnel data

37

Sharing with POST

Minn. Stat. § 626.8457

- Certain data must be shared with POST Board
 - LEAs must share public and private data on individual officers for peace officer database
 - Reporting obligation is ongoing; must be updated within 30 days of final disposition
 - Must cooperate with Board's licensing investigations and data requests
 - Must provide public and private data about alleged misconduct upon request
 - Confidential data must be shared if the Board requests it and needs it for their misconduct investigations

38

More miscellaneous provisions

- Security information, section 13.37
- Child maltreatment interview recordings, section 13.821
- Mental health data, section 13.46
- U-visa certification private data, section 611A.95, subd. 3.
- See also, Handout 206

39

Required LE policies and procedures

- Protected identities (Minn. Stat. §13.82 Subd. 17)
- BWC adoption (Minn. Stat. §626.8473)
- BWC access procedures (Minn. Stat. §13.825 Subd. 7(b))
- BWC biennial audit (Minn. Stat. §13.825 Subd. 9)
- UAV/drones (Minn. Stat. §626.19 Subd. 10)
- ALPR access procedures (Minn. Stat. §13.824 Subd. 7(b))
- ALPR biennial audit (Minn. Stat. §13.824 Subd. 6)
- Mental health and health records policy (Minn. Stat. §626.8477)
- Procedures for computer storage of peace officer records of children (Minn. Stat. §260B.171 Subd.5(a))
- <https://mn.gov/admin/data-practices/data/types/lawenforcement/policies/>

40



Law enforcement data scenarios, afternoon

Handout 204

Small Group Discussion



41