Minnesota Public Safety Answering Point and First Responder Personnel Training Procedure for Executive Order 20-34

On April 10, 2020, Governor Tim Walz issued Executive Order 20-34, *Protecting Minnesota's First Responders by Directing the Commissioner of Health to Share Information with the Department of Public Safety, 9-1-1 Dispatchers, and First Responders***.** In Executive Order 20-34 (EO 20-34), the Governor ordered the limited release of health data in connection with law enforcement, first responders and other public safety personnel and the COVID-19 pandemic. EO 20-34 requires various protections which are made operational by the corresponding protocol, which is incorporated in the Interagency Agreement for sharing of this data between the Minnesota Department of Health (MDH) and Minnesota Department of Public Safety/Emergency Communications Network (DPS/ECN).

Standard Operating Procedure for Private Health Data Entry

Following the *Tennessen* warning required by Minnesota Statutes section 13.04, subdivision 2, MDH will request the person to provide address information with sufficient detail to enable DPS/ECN to determine its validity. The *Tennessen* warning will advise the person of the purpose and use of collecting their location data. **The person may refuse to supply their address**. **MDH will not provide an address to DPS if the person has not been given a *Tennessen* warning or refused to provide their address.**

1. MDH will transmit the shared data related to positive COVID-19 cases within Minnesota via encrypted email to the DPS/ECN daily. The shared data must be associated with a full address (House Number, Street Name, Street Type, Directional, Apartment/Suite Number, City or Township, County) for each positive COVID-19 case.
    a. MDH will provide at least one staff contact to DPS/ECN in the event an address cannot be verified either by DPS/ECN or by the Public Safety Answering Point (PSAP). The MDH contact will review the database information and provide clarification when possible.
    b. DPS/ECN staff responsible for managing this data will sign a Confidentiality Agreement provided by the MDH. These will be retained by the ECN Director until 30 days after the expiration of EO 20-34.

2. DPS/ECN will sort the information by PSAP jurisdiction and transmit the appropriate record, based upon address, to the corresponding jurisdictional PSAP manager/designee via encrypted email on a daily basis. Each day following transmission, DPS/ECN will delete and remove from email "trash" folders the email from MDH and all accompanying emails and attachments to the PSAPs.

3. Designated PSAP staff will enter and retain the information associated with each MDH record as a premise file entry/informational entry into their Computer Aided Dispatch (CAD) systems associated with each address provided by MDH.

a. Designated PSAP staff responsible for managing this data will sign a Confidentiality Agreement provided by the MDH. These will be retained by each PSAP manager/designee until 30 days after the expiration of EO 20-34.
b. PSAPs will follow a screening protocol when feasible to identify if anyone at the address:
    i. is experiencing COVID-19 symptoms;
    ii. is COVID-19 positive; or
    iii. has been in contact with someone who is COVID-19 positive.

c. The following advisory statement will be entered into known private health data addresses: *"Based on screening and other information, assume the presence of COVID-19 at this address."*

This data shall be treated as private and shall be released only in accordance with the procedures outlined in the protocol.

Permission to Share Data

PSAPs will relay the advisory statement to a first responder only after exhausting other sources of information (*e.g.*, the screening protocol above) and when a first responder has an emergent need to know the shared data to aid in their infection control precautions. A first responder has an emergent need to know the shared data when the first responder:

1. Is dispatched to a location with an advisory statement entry;

2. Advises the PSAP they are responding to or arriving at a location with an advisory statement entry; or

3. Advises the PSAP they are self-initiating a call for service, attempting to serve legal papers or apprehend a person at a location with an advisory statement entry.

A first responder on scene at a location with an advisory statement may advise subsequent first responders arriving at the location of the advisory statement notification.

The "advisory statement" is the only COVID-19-specific health data from MDH that will be relayed to first responders by the PSAP.

Prior to entry at a location with an advisory statement notification, PSAPs will notify first responders by one of the following methods:

1. Mobile Data Computer (MDC) transmission
    a. 9-1-1 Telecommunicator will advise first responders to "check their MDC for important information."
2. By telephone when MDC is not available

a. 9-1-1 Telecommunicator will advise first responders who do not have an MDC to "call 9-1-1 center for important information."

3. By radio communication, only when neither MDC nor telephone are available to first responders. Any radio communication that could be monitored by the public or uninvolved parties shall be done using coded language or other similar methods to prevent the public or uninvolved parties from receiving the shared data.

First Responder Responsibility

Recipients of the shared data may use the information only for the limited purpose of protecting their health and that of other first responders making contact at an address.

No recipient of this shared data may use the information as a basis to refuse or delay a call for service or cause others to refuse or delay a call for service.

This shared data is "private" and shall be held to the same confidentiality standard as other confidential data (*e.g.*, CJIS) that is accessed and used within their daily course of business.

Record Management Retention

Shared data will be retained for each specific record for a period until which time MDH sends a cancelation file. The same process as defined in the Standard Operating Procedure for Private Health Data Entry outlined above shall be followed to purge records that are no longer active. All data will be deleted by the PSAP within 15 days of EO 20-34 being rescinded or the termination of the peacetime emergency.

Standard Operating Procedure for Private Health Data Removal

1. MDH will transmit the shared data related to positive COVID-19 cases within Minnesota that are no longer valid and are to be purged via encrypted email to the DPS/ECN daily. Private health data must be associated with a full address (House Number, Street Name, Street Type, Directional, Apartment/Suite Number, City or Township, County) for COVID-19 case to be purged.

2. DPS/ECN will sort the information by PSAP jurisdiction and transmit the appropriate records to be purged, based upon address, to the corresponding jurisdictional PSAP manager/designee via encrypted email on a daily basis. Each day following transmission, ECN will delete and remove from "trash" folders the email from MDH as well as all emails and attachments to the PSAPs.

    a. DPS/ECN staff responsible for managing this data will sign a Confidentiality Agreement provided by the MDH. These will be retained by the ECN Director until 30 days after EO 20-34 is rescinded or the termination of the peacetime emergency, whichever occurs first.

b. Removal files will be transmitted from DPS/ECN within eight hours of receipt by the MDH. Each PSAP shall purge the records within eight hours of receipt of the removal list from DPS/ECN.

Penalties

All PSAP employees and first responders shall be advised pursuant to Minnesota Statutes 2019, section 13.09(a), any person who willfully violates the provisions of the Minnesota Government Data Practices Act (MGDPA) or any rules adopted under the MGDPA or whose conduct constitutes the knowing unauthorized acquisition of not public data, as defined in section 13.055, subdivision 1, is guilty of a misdemeanor. In addition, pursuant to Minnesota Statutes 2019, section 13.09(b), willful violation of the MGDPA, including any action subject to a criminal penalty under the previous sentence, by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.