

records public databases Chapter 13 births  
word processing files tennessean warning storage  
adoption security requests identity fraud  
registration e-mail confidential complaints  
names addresses social security numbers paper  
law enforcement **Data Practices Notes for** front counter  
**Local Registrars** fax  
release not public access request court order  
subpoena certificates applicants insurance  
private calendars vendor attorney sanctions  
names mail Chapter 144 opinions contracts  
tangible interest fax government data steward  
MDH vital records databases Chapter 144 ROP  
local registrar marriages tangible interest  
storage security notarized registration  
funeral director fax names addresses phone  
state registrar signature MHS birth death  
certificate parent VRV2000 password county  
identity fraud file fees adoption fax  
expedite Chapter 13 confidential public

# 5 IMPORTANT DATA PRACTICES ITEMS TO REMEMBER



**Data are public UNLESS the law explicitly states otherwise.**



**Data practices laws are frequently changed. Be aware of the current requirements.**



**If you have questions or doubts, ASK your supervisor.**



**When dealing with people from outside MDH or the county on data practices matters, always clearly explain the reasons why the data are being collected or released or why the request for release is being denied.**



**Maintain written records of all requests for data.**

## Table of Contents

Introduction .....	1
Life Cycle of Government Data .....	1
Data Practices.....	1
Government Records and Records Retention .....	2
OSR & Local Registrar General Data Practices Requirements .....	3
Government Data.....	4
Data Protection and Security.....	5
Storing Data .....	6
Paper Files.....	6
Electronic Files.....	6
Viewing Public Vital Records.....	8
OSR Public Access Procedures for Viewing Public Birth and Death Information .....	8
Releasing Data.....	10
Office of the State Registrar and Local Registrars .....	10
Births .....	10
Fetal Deaths .....	12
Deaths .....	12
Subpoenas .....	13
Court Orders and Search Warrants .....	13
Releasing Data Flowchart .....	14
Data Practices Disputes and Questions .....	15

## Appendices

Appendix A: Glossary.....	16
Appendix B: Persons with Data Practices Related Responsibilities .....	18
Appendix C: Data Classifications for Copies of Vital Records.....	19
Appendix D: Data Classifications for Copies of Documents Related to a Vital Record ..	20

# Introduction

---

## Life Cycle of Government Data

---

The following table provides the statutory cites that apply to **government data/government records** over the course of the life cycle of the data/record.

Create and maintain	Creation of data	Official Records Act	Minnesota Statutes, section 15.17
Use and disclose	Life of the data	Data Practices Act	Minnesota Statutes, chapter 13
Dispose	End of data	Records Management Statute	Minnesota Statutes, section 138.17

The life cycle of **government data** involves data practices, **government records**, and records retention. Although **government data** and **government records** are very similar, they are not identical, and it is important to distinguish between the two issues. All recorded information regardless of the media (e.g., paper, microfilm, electronic storage) is considered **government data**. Certain types of **government data** are not considered **government records**. There are definitions of **government data** and **government records** in the Glossary in Appendix A. Additionally, Section II of this manual provides guidelines for determining when **government data** are considered **government records**.

## Data Practices

---

The Minnesota Government Data Practices Act, Minnesota Statutes, chapter 13, which requires public agencies to:

- 1) safeguard the privacy rights of **data subjects** about whom state and local governments collect, store, and use data; and
- 2) facilitate access to all **government data** which should be rightfully disclosed.

All Office of the **State Registrar (OSR)** and **Local Registrar** staff must comply with the Minnesota Government Data Practices Act. Chapter 13 applies to all government programs that collect data. In addition, **OSR** has specific statutory authority or requirements pertaining to data practices. How you use and maintain the data will vary depending on how the data are classified. Your supervisor is responsible for the security of data your program collects and maintains. When the statutes allow it, your supervisor may authorize data access to you, other **Local Registrar** or **OSR** staff, and the staff

of other agencies or private entities. As staff who may be responsible for program data, you must familiarize yourself with how data are classified and when and to whom data can be released.

This document will help to guide you in collecting, processing, storing, and releasing or not releasing data to those who may request access to data you maintain.

## **Government Records and Records Retention**

---

The Official Records Act, Minnesota Statutes, section 15.17, require government entities to “make and preserve all records necessary to a full and accurate knowledge of their official activities.” the Records Management Statute, Minnesota Statutes, section 138.17, require the establishment of an active, continuing program for economical and efficient management of **government records**.



**Data are public UNLESS the law explicitly states otherwise.**

# DATA PRACTICES

## OSR & Local Registrar General Data Practices Requirements

- 1) All data collected, created, received, maintained, or disseminated by **OSR** and a **Local Registrar** are public unless otherwise classified by statute.
- 2) Before collecting **private and confidential data** on **individuals**, you must inform them of their rights using a **Tennessee warning**.
- 3) You must only release **private, confidential, nonpublic**, and **protected nonpublic data** under the conditions described in this document. If you receive **not public data** that you did not request or is not required, you must destroy it or return it to the person or entity who submitted it.
- 4) If you violate the provisions of the Minnesota Government Data Practices Act you may be subject to disciplinary action and/or civil penalties.
- 5) You must complete data practices training as directed by your supervisor. Your training will include specific information about the data maintained by your program. This training is provided by **OSR**. A **Local Registrar** or other county staff or staff from the Department of Administration and the Office of the Attorney General may also provide training opportunities.
- 6) You must refer non-routine data practices questions to your supervisor. Don't guess—get a second or third opinion if you are in doubt of the status of the data in question.
- 7) Your county must maintain a list of the data you collect or maintain that are **private or confidential**. The list must include statutory references defining it as **private or confidential**. The document must also contain copies of the forms you use to collect this data.



**Data practices laws are frequently changed.  
Be aware of the current requirements.**

## GOVERNMENT DATA

All data kept in any recorded form, regardless of physical form, storage media, or conditions of use

Classification		Definition	Who has Access	Examples
<i>Data on Individuals</i>	<i>Data not on Individuals</i>			
<b>Public</b>	<b>Public</b>	All <b>government data</b> unless specified by law	Anyone for any reason	<p><b><u>Public Data on Individuals:</u></b> Death records</p> <p><b><u>Public Data Not on Individuals:</u></b> Names and Locations of Local Registrar Offices</p>
<b>Private</b>	<b>Nonpublic</b>	Accessible to <b>data subject</b> and not public	<b>Data subject</b> or <b>authorized representative</b> ; no public access; and only those <b>MDH</b> employees with a “need to know”	<p><b><u>Private: Health information</u></b> on the birth record; social security numbers</p> <p><b><u>Nonpublic:</u></b> Specific security information about MN VRV2000</p>
<b>Confidential</b>	<b>Protected Nonpublic</b>	Not public and not accessible to <b>data subject</b>	Only those <b>MDH</b> employees with a “need to know”	<p><b><u>Confidential:</u></b> Birth records for births to unmarried parents; Original births records after an adoption</p> <p><b><u>Protected Nonpublic:</u></b> Data on agencies that is part of an open investigation</p>
<p><b>Not Public Data</b> is a broad category of data that includes <b>confidential, private, nonpublic, and protected nonpublic data.</b></p>				
<p>Statutory Reference: Minnesota Statutes, section 13.02</p>				

# **Data Protection and Security**

To comply with the Minnesota Government Data Practices Act and adequately protect **OSR** and **Local Registrar** data assets, you must:

- 1) Put away **not public data** when you leave your desk and close files that contain **not public data** when being visited. **Not public data** and files include information that describes **not public data** such as documentation or data dictionaries.
- 2) Make copies of **not public data** only when necessary and shred copies when they are no longer needed. Please check with your administrative support staff regarding shredding procedures.
- 3) Comply with the network and data handling security policies established by **OSR** and by your county.
- 4) Keep **not public data** behind two locks, such as behind a security door and a locked file cabinet or password. For especially sensitive data, additional safeguards may be warranted.
- 5) Use applicable data classifications and statutes to determine if and how data can be released.
- 6) Seek advice from your supervisor when in doubt about data classification or security.



**If you have questions or doubts, ASK your supervisor.**

# Storing Data

---

*Statutory Reference: Minnesota Statutes, section 13.03, subdivisions 1 and 3.*

Remember that all the data we store could be requested. You must store data in a manner that will facilitate retrieval. To determine the appropriate media, consider the characteristics of your data and the size and frequency of the requests you expect to receive. Paper, microfilm, microfiche, or electronic media may be appropriate. It depends on the data.

Use current reliable documentation or applicable statutes to determine data classification and retention schedule and store data accordingly. If in doubt about data classification, retention schedule, or required security, seek advice from your supervisor. Remember that you will not be able to charge for the separation of **not public data** from **public data** when the data are requested.

## Paper Files

---

- 1) Keep files that contain **not public data** behind two locks, such as the locked entrance door and a locked file cabinet.
- 2) Put away **not public data** when you leave your desk. Close files that contain **not public data** when being visited.
- 3) Pick up print outs and faxes that contain **not public data** immediately.
- 4) Print or copy **not public data** only when necessary and shred copies when they are no longer needed. Please check with your administrative support staff regarding shredding procedures.

## Electronic Files

---

- 1) Limit your access to data that you need to do your daily work. Cooperate with the **OSR** and others in your county in defining the appropriate level of access.
- 2) Store files in a manner that reduces the possibility of errors, file corruption, and unauthorized access.
- 3) Store data in a manner appropriate to their classification. For example, data sets that include **not public data** must have additional password protection. For especially sensitive data, additional safeguards may be warranted.
- 4) Store data in a software format (e.g., database, spreadsheet, analysis tool) that will facilitate secure storage and efficient processing.
- 5) Limit the number of copies of a data set or partial data set. Ensure that all changes to data sets are documented and made on the appropriate version.

- 6) Document data so the potential uses and limitations of the data are clear.
- 7) Use passwords (login, screensaver, and GroupWise) that meet or exceed the standards set by the Center for Health Statistics. If you have questions about these standards, please contact your computer support staff;
- 8) Store files in the appropriate location on network drives so that access to the data will be controlled and the data will be backed up and secure. Do not store **not public data** on your C: drive, on diskettes, or on any local drive;
- 9) Use file transfer methods that meet or exceed the standards set by the Center for Health Statistics. If you have file transfer needs, please contact your computer support staff;
- 10) If you take a laptop out of the office, know what files are stored on the laptop and the level of security you must maintain; and
- 11) If you use a personal digital assistant (PDA), comply with the PDA use policies set by your county.



**If you have questions or doubts, ASK  
your supervisor.**

# Viewing Public Vital Records Data

---

*Statutory Reference: Minnesota Statutes, section 13.03, subdivisions 2 and 3, section 13.05, subdivision 12, and section 144.225, subdivision 1*

A requester must be allowed to view public data without charge. A requester is not required to give identifying information. **OSR** and **Local Registrars** must:

- 1) regulate physical access to **vital records** in order to protect **vital records** from loss, mutilation or destruction and to prevent improper disclosure of **vital records** which are **confidential or private data** on **individuals**;
- 2) establish procedures, consistent with Minnesota Statutes, chapter 13 to insure that requests for **government data** are received and complied in an appropriate and prompt manner. A person must be able to view public **government data** at reasonable times and places and staff must be available to answer questions about the data;
- 3) prepare written public access procedures and update them no later than August 1 of each year as necessary to reflect any changes in personnel or circumstances that might affect public access to **government data**; and
- 4) make copies of the written public access procedures easily available to the public through distribution or posting a copy of the procedures in a conspicuous public place

## OSR Public Access Procedures for Viewing Public Birth and Death Information

Viewing one record: A person who comes into the office to view public birth or death information is required to complete an application. Staff use the application to locate the record or related information, ensure that the information is public, and provide a noncertified copy of the public record or related information. The person views the copy of the record or related information in the reception area. After the person views the copy of the record or related information, the person may purchase the copy by paying the fee for a noncertified copy of the record or the fee for a documented related to a **vital record**. If the person does not purchase the noncertified copy of the record or related information, each copy is destroyed.

Viewing more than one record: If the persons wishes to view more than one record, **OSR** staff will evaluate the request based on the volume of records or related information to be viewed and the ability of the person to provide sufficient information to easily locate the records or related information. If feasible, **OSR** staff will use the procedure described above for viewing one record. **OSR** reserves the right to require the person to make an appointment. When a person has an appointment, **OSR** staff will escort the person to the search area and locate the records and related information the person wants to view. **OSR** staff ensure that the records to be provided to the person to view are public. The person views the records. **OSR** staff will remain present to protect the records from loss or destruction and to answer any questions about the records and related information.

Future plans include making a computer work station available to the general public at the **OSR** for searching and viewing public records electronically.

**MDH** also has written access procedures for public access to **MDH** data. These procedures are in a document titled Minnesota Department Of Health (**MDH**) Data Practices Policy: Information For The Public About Public Access To **MDH** Data And Rights Of **Data Subjects**. A copy of this document can be found on the Internet at <http://www.health.state.mn.us/divs/opa/datapolicy.rtf> or through the **MDH** home page. On the left side of the **MDH** home page, click on "information & resources," scroll about half way down the page. The policy link is in the second bullet under "Minnesota public health policy and regulations."



**When dealing with people from outside MDH or the county on data practices matters, always clearly explain the reasons why the data are being collected or released or why the request for release is being denied.**

# Releasing Data

---

## Office of the State Registrar and Local Registrars

---

*Releasing Data Governed by the Vital Statistics Act, Minnesota Statutes, sections 144.211 to 144.227, and Minnesota Rules, chapter 4601*

### Births

---

Each birth records has two parts. One part is ***civil registration information***, which is needed to register the birth in Minnesota. Generally, the ***civil registration information*** includes the baby or registrant's name, the parents' names, and information about the date and place of birth. The second part of the birth record is the ***health information***. ***Health information*** is collected for each birth for statistical purposes. Generally, ***health information*** includes race and education information about the parents, and information about pre-natal care and the delivery.

Birth records are classified according to Minnesota Statutes, section 144.225. For most births, the ***civil registration information*** on the birth record is public. However, for births to unmarried parents, the ***civil registration information*** on the birth record is confidential, unless the mother has designated the record as public. Subdivision 2 allows release of the confidential birth record:

- (1) to a parent or guardian of the child;
- (2) to the child when the child is 16 years of age or older; or
- (3) pursuant to a court order.

Additionally, the name and address of a mother and the child's date of birth may be disclosed to the county social services or public health member of a family services collaborative. Additionally, under certain circumstances, confidential birth records may be released to the Department of Human Services.

Unless the child is adopted, data pertaining to the birth of a child become public data if 100 years have elapsed since the birth of the child who is the ***data subject***. Or, if the ***data subject*** has died or is presumed dead, then the data may be released when ten years have elapsed from the actual or presumed death of the ***individual*** and 30 years have elapsed from the creation of the data.

The ***health information*** part of the birth record is classified as ***private data*** by Minnesota Statutes, section 144.225, subdivision 2a. The mother is generally considered to be the ***data subject*** of the ***health information***. Limited information may be released to the registrant or to the father. In certain circumstances, ***health information*** may also be shared with local health agencies and the Department of Human Services.

Birth Certificates. Certified birth records (i.e., birth certificates) are used for legal purposes such as to enroll in school, to prove identity to obtain a driver's license or passport, or to apply to the Social Security Administration for retirement benefits. To help protect each person's identity, there are restrictions on the release of birth certificates in addition to the release allowed by the classification of the data. Minnesota Statutes, section 144.225, subdivision 7, require evidence of tangible interest before a birth certificate can be released.

A person has a **tangible interest** if the person is:

- 1) the registrant (**data subject** of the birth record);
- 2) a child of the registrant;
- 3) the spouse of the registrant;
- 4) a parent of the registrant;
- 5) the grandparent or grandchild of the registrant;
- 6) the party responsible for filing the birth record;
- 7) the legal custodian or guardian or conservator of the registrant; or
- 8) a licensed attorney.

Persons may also be considered to have **tangible interest** if they can demonstrate that they need the certificate for the administration of an estate or for the determination or protection of a personal or property right. Organizations such as adoptions agencies and government agencies may also be considered to have **tangible interest** in certain circumstances.

Demonstrating **tangible interest** does not allow the release of private or confidential information.

Documents related to birth records. The classification and release of an **affidavit** to amend, an application to amend, or documentation for a delayed registration is the same as the classification and release of the record amended or created. For example an application to amend a public birth record is public and may be released to anyone who requests a copy. If **health information** on the birth record is amended the **affidavit** or application to amend is private and may be released to the **data subject**. Documents related to amending or creating a confidential birth record are confidential and may be released with the same limitations as the confidential birth record.

Establishment of Paternity and Adoption. The Department of Human Services is the lead agency on the statutes, rules, and procedures for the establishment of paternity and adoption. **OSR** staff process documents related to registering or replacing the birth record such as Recognition of Parentage, husband's non-paternity statements, **affidavits** of disclosure and nondisclosure regarding an adoption, and **affidavits** to retain parental rights.

A Recognition of Parentage (ROP) and a husband's non-paternity statement are classified as **confidential data** related to a birth to unmarried parents. Minnesota Statutes, section 257.73, subdivision 3, which apply to replacement records, classify these data as confidential, released with consent of the court and all interested persons, or a court order. Section 144.225, subdivision 2, allows ROPs and non-paternity statements to be released in the same manner as a confidential birth record.

Minnesota Statutes, section 144.218, classify birth records that are replaced because paternity has been established or because of an adoption as **confidential data**. Documents related to the replacement are also confidential. The original birth record may be released on consent of the court and the consent of all interested parties or upon a court order. Parents named on the original birth record may give their permission to release information from the original birth record to the registrant.

## Fetal Deaths

---

Fetal death reports are collected for statistical purposes only. Fetal deaths are not registered and fetal death certificates are not issued. A fetal death report has basically the same parts as a birth record. One part is classified as public and includes the name of the fetus if applicable, the parents' names, and information about the date and place of the fetal death. The second part of the fetal death report is classified as private and includes **health information**. Generally, **health information** includes race and education information about the parents, and information about pre-natal care and the delivery.

## Deaths

---

Each death records has two parts. One part is the **fact of death information**, which is needed to register the death in Minnesota. Generally, the **fact of death information** includes the name of the deceased, information about the date, time, and place of death, and other information about the deceased. The second part of the death record is the cause of death. Cause of death information is medical information about the factors that caused or contributed to the person's death.

Death records are classified according to Minnesota Statutes, section 144.225. All death records are public.

Death Certificates. Certified death records (i.e., death certificates) are used for legal purposes such as collecting life insurance or for the administration of an estate. To help reduce fraudulent uses of death certificates, there are restrictions on the release of death certificates. Minnesota Statutes, section 144.225, subdivision 7, require evidence of **tangible interest** before a death certificate can be released.

A person has a **tangible interest** if the person is:

- 1) a child of the deceased;
- 2) the spouse of the deceased;
- 3) a parent of the deceased;
- 4) a sibling of the deceased;
- 5) the grandparent or grandchild of the deceased;
- 6) the party responsible for filing the death record;
- 7) the legal custodian or guardian or conservator of the deceased; and
- 8) a licensed attorney.

Persons may also be considered to have **tangible interest** if they have been identified by the funeral director who filed the death record, or if they demonstrate a need for the certificate for the administration of an estate or trust; or for the determination or protection of a personal or property

right Government agencies may also be considered to have **tangible interest** in certain circumstances.

## **Subpoenas**

---

*Rules and Statutory Reference: Minnesota Rules, part 1205.0100, subpart 5, Minnesota Statutes, section 13.03, subdivision 6, and Minnesota Statutes, section 144.225, subdivision 7, paragraph (a), clause (4)*

A subpoena in and of itself is not a court order allowing for the release of **not public data**. If you are served with a subpoena requesting the release of **not public data**, the data should not be released. Submit all subpoenas to the **Local Registrar** immediately. The **Local Registrar**, with legal advice, will inform the court about the statutory provision restricting the disclosure of the data.

If you receive a call about a subpoena, instruct the caller to address the subpoena as you are instructed by your **Local Registrar**. Report the call to your supervisor.

## **Court Orders and Search Warrants**

---

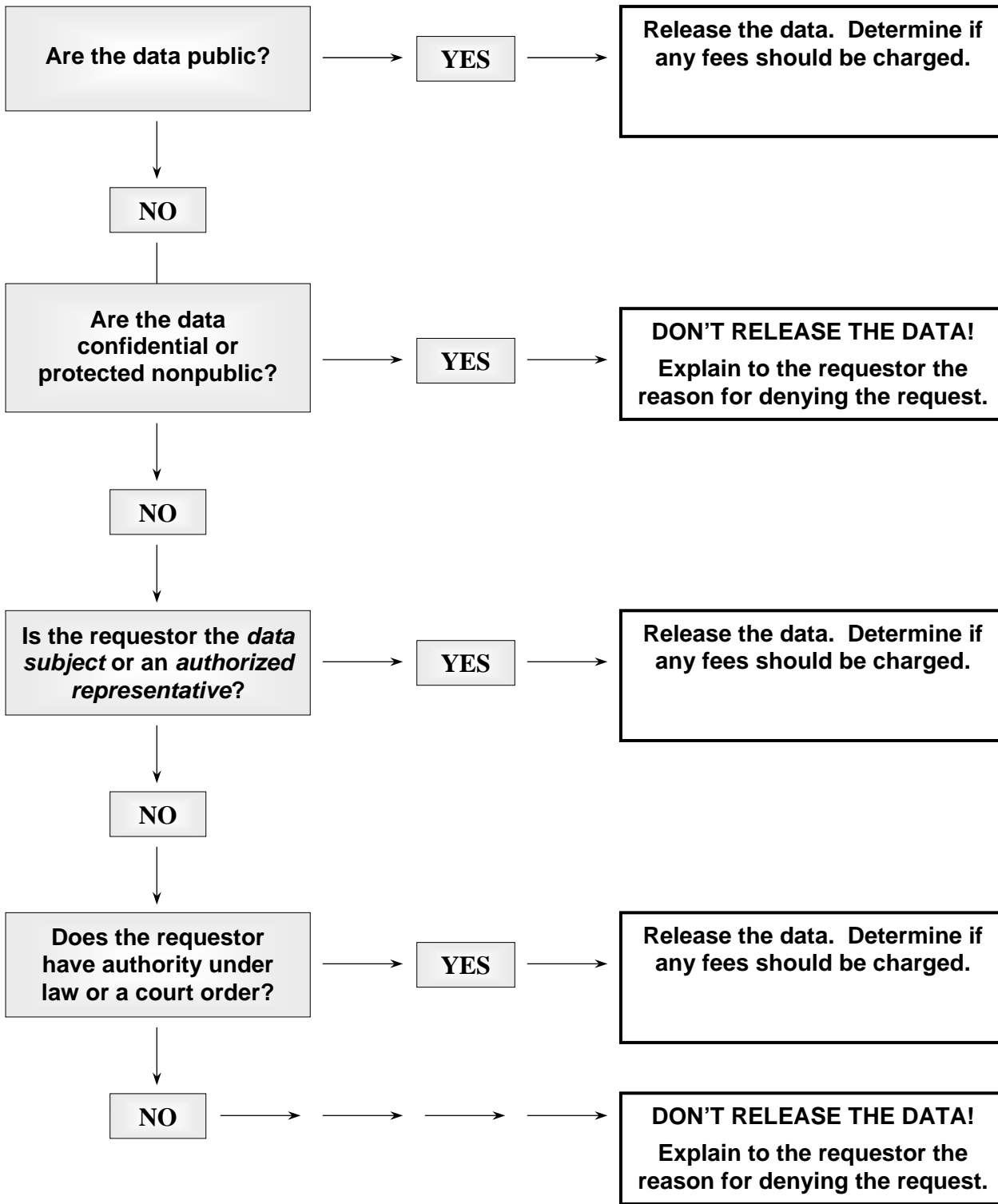
**Not public data** may be released pursuant to a court order or search warrant. Court orders and search warrants are signed by a judge of either a state or federal court and specify the data to be released. If presented with a court order or search warrant, contact your supervisor or the **Local Registrar** immediately. Your supervisor and the **Local Registrar** will determine if the data will be released. There may be a basis on which the **Local Registrar** opposes its release. If that is the case, your county attorney general may provide counsel.



**Maintain written records of all requests for data.**

# RELEASING DATA

## Minnesota Government Data Practices Act



# Data Practices Disputes and Questions

---

*Statutory Reference: Minnesota Statutes, section 13.072.*

Government entities or **individuals** seeking resolution of disputes relating to Minnesota Statutes, chapter 13 and other statutes regulating **government data** practices may request an advisory opinion from the Commissioner of Administration. Advisory opinions may also be requested on any question concerning access to **government data**, the rights of **data subjects**, or the classification of data.

An advisory opinion is not binding. However, a court must give deference to the opinion in a proceeding that involves the data dispute and a government entity or **individual** that conforms with an opinion will not be liable for damages

To request an advisory opinion, send a written request to:

Commissioner of Administration  
c/o Information Policy Analysis Division  
305A Centennial Building  
658 Cedar Street  
St. Paul, Minnesota 55155  
Fax: 651-205-4219

For additional information or copies of previously issued opinions, call 651-296-6733 or visit the Department of Administration web site at <http://www.ipad.state.mn.us>.

## Appendix A Glossary

**Affidavit.** A written declaration or attestation that is signed before a notary public.

**Authorized Representative.** Any *individual* authorized in writing by a *data subject* to receive *government data* about the *data subject*.

**Civil Registration Information.** The portion of the birth record describing the registrant and the date and place of birth (Reference: Minnesota Rules, part 4601.0100, subpart 5).

**Confidential Data.** Data on an *individual* that are (a) not public and (b) not available to the *individual* (Statutory Reference: Minnesota Statutes, section 13.02, subdivision 3).

**Data Subject.** *Individual* or entity about whom data are collected or maintained. One record may have multiple *data subjects*.

**Fact of Death Information.** Information required by the *state registrar* to record the time and place a death occurs and to identify the person who is deceased (Reference: Minnesota Rules, part 4601.0100, subpart 11).

**Government Data.** All data, information, or records collected, created, received, maintained, or distributed by public agencies regardless of its physical form, storage media, or conditions of use. *Government data* includes data received from secondary sources including data downloaded from the Internet (Statutory Reference: Minnesota Statutes, section 13.02, subdivision 7).

**Government Records.** All state and local information or documentary material, regardless of physical form or characteristics, storage media or conditions of use, made or received pursuant to state law or in connection with the transaction of public business by a state or local officer or agency (Statutory Reference: Minnesota Statutes, section 138.17, subdivision 1).

**Health Information.** Medical or statistical information from which an identification of risk for disease, disability, or developmental delay in a mother or child can be made (Reference: Minnesota Rules, part 4601.0100, subpart 14).

**Individual.** A person. For a minor (person under 18) or an *individual* judged mentally incompetent, it can be a parent or guardian. You may withhold data from a parent or guardian if the minor requests and if it is in the best interest of the minor (Statutory Reference: Minnesota Statutes, section 13.02, subdivision 8).

**Local Registrar.** An individual designated under Minnesota Statutes, section 144.214, subdivision 1 to perform the duties described in section 144.214 and in Minnesota Rules, 4601.0300. (Statutory Reference: Minnesota Statutes, section 144.212, subdivision 10).

**MDH.** The Minnesota Department of Health.

**Nonpublic Data.** Data not on *individuals* that are (a) not public and (b) accessible to the *data subject*. Also information about information systems and networks that might be used to compromise this data (Statutory Reference: Minnesota Statutes, section 13.02, subdivision 9).

**Not Public Data.** A broad category of data that includes *confidential, private, nonpublic, and protected nonpublic data* (Statutory Reference: Minnesota Statutes, section 13.02, subdivision 8a).

**OSR.** The Office of the *State Registrar* as established in Minnesota Statutes, section 144.213. The Office of the *State Registrar* is a program of the Center for Health Statistics, Office of Health Policy Statistics and Informatics, Minnesota Department of Health.

**Private Data.** Data on an *individual* that are (a) not public and (b) accessible to the *individual* (Statutory Reference: Minnesota Statutes, section 13.02, subdivision 12).

**Protected Nonpublic Data.** Data not on *individuals* that are (a) not public (b) not accessible to the *data subject* (Statutory Reference: Minnesota Statutes, section 13.02, subdivision 13).

**Public Data.** Data accessible to anyone for any reason (Statutory Reference: Minnesota Statutes, section 13.02, subdivisions 14 and 15).

**Security Information.** *Government data* that the disclosure may jeopardize the security of information, possessions, *individuals* or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury. *Security information* includes documentation of *MDH* computer systems security. *Security information* is classified as nonpublic (for data not on *individuals*) and private (data on *individuals*) (Statutory Reference: Minnesota Statutes, section 13.37, subdivisions 1a and 2).

**State Registrar.** A designee of the Commissioner of Health who is responsible for the administration of the *system of vital statistics* (Statutory Reference: Minnesota Statutes, section 144.213, subdivision 2).

**System of Vital Statistics.** The processing of the registration, collection, preservation, amendment, and certification of *vital records* and related activities (Statutory Reference: Minnesota Statutes, section 144.212, subdivision 7).

**Tangible Interest.** Criteria established in Minnesota Statutes, section 144.225, subdivision 7 to control issuance of certified birth and death records including certified statements of no record found.

**Tennessee Warning.** A notice you must give to an *individual* who is asked to supply *private or confidential data* about himself or herself (Statutory Reference: Minnesota Statutes, section 13.04, subdivision 2).

**Vital Record.** A record or report of birth, death, marriage, dissolution and annulment, and related data (Statutory Reference: Minnesota Statutes, section 144.212, subdivision 8).

**Vital Statistics.** The data derived from records and reports of birth, death, fetal death, induced abortion, marriage, dissolution and annulment, and related reports (Statutory Reference: Minnesota Statutes, section 144.212, subdivision 9).

## Appendix B

# Persons with Data Practices Related Responsibilities

**Responsible Authority.** The responsible authority for **MDH** is the Commissioner. The responsible authority for **OSR** is the **State Registrar**. The responsible authority for your county is appointed by your county board. The responsible authority must ensure the agency complies with the Data Privacy Act. Responsibilities include the collection, use, and dissemination of any set of data on **individuals**, **government data** or **summary data**, and the implementation and administration of the Act. The duties of the responsible authority are detailed in statute and rule (Statutory and Rule Reference: Minnesota Statutes, section 13.02, subdivision 16 and section 13.05, and Minnesota Rules, chapter 1205).

**Data Practices Compliance Official.** The data practices compliance official is designated by the Responsible Authority to be the agency or county contact for data practices. Anyone may direct questions or concerns regarding problems in obtaining access to data or other data practices problems to the data practice compliance official. The data practices compliance official will help to establish data practices policies for the agency or county and provide training. Dave Orren is the **MDH** Data Practices Compliance Official (Statutory Reference: Minnesota Statutes, section 13.05, subdivision 13).

**Designee.** A designee is a person appointed in writing by the Responsible Authority to be in charge of individual files or systems containing governmental data, and to comply with requests for governmental data (Statutory Reference: Minnesota Statutes, section 13.02, subdivision 6).

**Employee.** Each employee is responsible for compliance with the Data Privacy Act. Willful violation of chapter 13 by any employee constitutes just cause for suspension without pay or dismissal (Statutory Reference: Minnesota Statutes, section 13.03, section 13.08, subdivision 1, and section 13.09 ).

**Commissioner of Administration.** In 1993, the legislature granted the Commissioner of the Department of Administration the authority to issue written advisory opinions, upon request of any person, on questions of public access to governmental data, rights of **data subjects**, and classifications of data. Opinions issued by the Commissioner of Administration are not binding on the state agency, but must be given deference by a court in a proceeding involving the data. The Commissioner of the Department of Administration also grants or denies requests for a temporary classification of data (Statutory Reference: Minnesota Statutes, section 13.072).

**The Attorney General.** A formal written opinion by the Attorney General takes precedence over an advisory opinion of the Commissioner of the Department of Administration. Agency staff may seek informal advice from attorneys in the Office of the Attorney General on data practices issues but informal advice is not entitled to any precedential value in a legal dispute (Statutory Reference: Minnesota Statutes, section 13.072, subdivision 1, paragraph f).

**The Courts.** The Act creates a procedure for when data that is not public can be released by Court order. The Act affords remedies to **individuals** who maintain that a governmental agency is violating or not properly administering the provisions of the Act. Agencies who violate the Act and cause damage to an **individual** can be sued. The **individual** may recover actual damages, costs and attorney fees. In cases of willful violations, the **individual** may recover up to \$10,000 in exemplary damages. Any person who willfully violates the provisions of chapter 13, or Minnesota Rules, chapter 1205 is guilty of a misdemeanor (Statutory Reference: Minnesota Statutes, section 13.03, subdivision. 6, section 13.08, subdivision 1, and section 13.09 ).

## Appendix C

### Data Classification for Copies of Vital Records

Document	Classification	Minnesota Statutes Reference
Birth Record- <b><i>civil registration information</i></b>	<p>Public for all birth records <u>except records for births to unmarried parents, which are confidential unless designated public by the mother.</u> Confidential birth records may be released only to the parent or guardian, child at age 16 or older, or with a court order.</p> <p>Unless the child is adopted, data pertaining to the birth of a child become public data if 100 years have elapsed since the birth of the child who is the <b><i>data subject</i></b>. Or, if the <b><i>data subject</i></b> has died or is presumed dead, then the data may be released when ten years have elapsed from the actual or presumed death of the <b><i>individual</i></b> and 30 years have elapsed from the creation of the data.</p>	144.225, subdivisions 1 and 2
Birth Record- <b><i>health information</i></b>	Private for all birth records. Information can only be released to the <b><i>data subject</i></b> . The mother is generally considered to be the <b><i>data subject</i></b> of the <b><i>health information</i></b> . Limited information may be released to the registrant or to the father. For example the father's social security number, race, and education may be released to the father.	144.225, subdivision 2a
Death Record	Public for all deaths. May be released upon request. Please note that tangible interest applies to certified death certificates.	144.225, subdivision 1
Fetal Death Report	Public except for the <b><i>health information</i></b> section, which is private. The mother is generally considered to be the <b><i>data subject</i></b> of the <b><i>health information</i></b> . Limited information may be released to the father. For example the father's race, and education may be released to the father.	144.225, subdivision 1 144.225, subdivision 2a
Statement of No Record Found	Public. Please note that tangible interest applies to certified Statements of No Record Found.	144.225, subdivision 1

Note: ***Tangible interest*** as defined in Minnesota Statutes, section 144.225, subdivision 7, applies to the release of birth and death certificates (i.e., certified copies of birth and death records).

## Appendix D

### Data Classifications for Copies of Documents Related to a Vital Record

Documents Related to a <i>Vital Record</i>	Related to:	Classification	Minnesota Statutes Reference
Certified copy of a recognition of parentage (ROP) or a husband-s non-paternity statement	Birth Record	Confidential - Minnesota Statutes, section 257.73, subdivision 3, apply to replacement records and classify these data as confidential, released with consent of the court and all interested persons, or a court order. Section 144.225, subdivision 3, allows ROPs and non-paternity statements to be released in the same manner as a confidential birth record.	Section 144.225, subdivision 2 Section 257.73, subdivision 3
<b>Affidavits</b> of disclosure regarding an adoption	Birth Record	Confidential Generally, an <b>affidavit</b> of disclosure regarding the release of original birth record information after an adoption is not released. A noncertified copy of the original birth record or the information is released.	Section 259.83
<b>Affidavits</b> of nondisclosure regarding an adoption	Birth Record	Confidential The <b>affidavit</b> of nondisclosure regarding the release of original birth record information after an adoption is not released. A letter stating that the birth record information cannot be released is sent to the requester. A similar letter is sent if there is no <b>affidavit</b> found.	Section 259.83
<b>Affidavit</b> to retain parental rights	Birth Record	Confidential used to notify the other parent; applies to births that occurred before January 1, 1998	Section 259.51 (repealed 1997)
<b>Affidavit</b> or application to amend a birth or death record	Birth or Death Record	Same classification as the record amended. See table in Appendix C.	Section 144.225, subdivisions 1 and 2