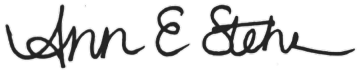
HOSPICE
of Douglas County
A division of
Horizon Public Health

809 Elm Street Suite 1200
Alexandria, MN 56308
320.763.6018 | 800.450.4177
320.763.4127 fax
hospicedouglascounty.org

Policy Title:	MN DATA PRACTICES POLICY				
Administrator Signature:			**Approved Date:**	01.01.2015	
Effective Date:	07.10.2023				
Reviewed Date:	06.15.2023	**Revision Approved Date:**	07.10.2023	**Policy Version:**	
Reviewed Date:		**Revision Approved Date:**		**Policy Version:**	

Policy Statement: The Minnesota Government Data Practices Act (MGDPA) is a state law that controls how government data is collected, created, stored, maintained, used and disseminated. It is the policy of Horizon Public Health (HPH) to collect and manage government data in accordance with Minnesota laws.

Purpose Statement: These guidelines and procedures provide direction in complying with those portions of the MGDPA that relate to public access to government data and to the rights of subjects of the data.

Statutory References:

Minnesota Government Data Practices Act

Minnesota Statutes Chapter 13
Minnesota Rules, parts 1205.0100 to 1205.2000

Official Records

Minnesota Statutes § 15.17

Destruction of Records

Minn. Stat. §§ 138.163 and 138.17

U. S. Code

18 U.S. Code § 2721 – Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records

Table of Contents

Introduction

These guidelines and procedures provide direction in complying with those portions of the MGDPA that relate to *public access to government data* and to the *rights of subjects of data.*

The public access requirements are:

- The presumption that all government data are public unless classified as not public by state or federal statute;
- The right of any person to know what kinds of data are collected by the government entity and how that data is classified;
- The right of any person to inspect, at no charge, all public government data at reasonable times and places;
- The right of any person to have public data explained in an understandable way;
- The right of any person to get copies of public government data at a reasonable cost;
- The right of any person to an appropriate and prompt response from the government entity when exercising these rights; and
- The right of any person to be informed of the authority by which an entity can deny access to government data.

A BRIEF OVERVIEW
OF THE
MINNESOTA GOVERNMENT DATA PRACTICES ACT

The Minnesota Government Data Practices Act regulates the management of all government data that are created, collected, received, or released by a government entity, no matter what form the data are in, or how they are stored or used.

Briefly, the Act regulates:

- what data can be collected;
- who may see or get copies of the data;
- the classification or specific types of government data;
- the duties of government personnel in administering the Act;
- procedures for access to the data;
- procedures for classifying data as not public;
- civil penalties for violation of the Act; and
- the charging of fees for copies of government data.

Government data is either *data on individuals or data not on individuals*. Data on individuals are classified as either public, private, or confidential. Data not on individuals are classified as public, nonpublic, or protected nonpublic. The classification system determines how government data are handled (see chart below).

Data on Individuals	**Meaning of Classification**	**Data <u>Not</u> on Individuals**
Public	Available to anyone for any reason	Public
Private	Available only to the data subject and to anyone authorized by the data subject or by law to see it	Nonpublic
Confidential	Not available to the public or the data subject.	Protected Nonpublic

I. COLLECTION OF GOVERNMENT DATA

Government data is all data maintained in any recorded form by government entities, including counties. As long as data is recorded in some way by a government entity, it is government data, no matter what physical form it is in, or how it is stored or used. Government data may be stored on paper forms/records/files, in electronic form, on audio or video tape, on charts, maps, etc. Government data normally does not include mental impressions.

Official records must be kept as set forth under Minn. Stat. § 15.17, Subd. 1, which requires all officers and agencies of the state, and all officers and agencies of the counties, cities, and towns to make and keep all records necessary for a full and accurate knowledge of their official activities. Requirements for collecting, creating, maintaining, storing, and disseminating data are found in Minnesota Chapter 13 and Minnesota Rules 1205.

Links for locating the governing statute and rules are below:

Minnesota Chapter 13 – Government Data Practices
https://www.revisor.mn.gov/statutes/?id=13

Minnesota Administrative Rules, Chapter 1205, Data Practices
https://www.revisor.mn.gov/rules?id=1205

The collection and storage of public, private and confidential data on individuals is limited to that necessary for the administration and management of programs specifically authorized or mandated by the state, local governing body, or the federal government.

II. DEFINITIONS

A. Data Inventory: The public document which is required by Minn. Stat. § 13.025, Subd. 1, containing the name of the responsible authority and the individual designee, title and address, and a description of each category of record, file or process relating to private or confidential data on individuals maintained by the government entity. The responsible authority shall update the inventory annually and make any changes necessary to maintain the accuracy of the inventory.

B. Authorized Representative: The individual, entity, or person authorized to act on behalf of another individual, entity or person. For the purposes of the Act, the authorized representative may include, but is not limited to: (a) in the case of a minor, a parent, or guardian, (see Section IX.B, Notification of Minors); (b) an attorney acting on behalf of an individual when the individual has given written informed consent; (c) any other individual entity, or person given written authorization by the data subject; or (d) an insurer or its representative, provided that the data subject has given informed consent for the release of the information, (e) court appointed guardian/conservator.

C. Court Order: The direction of a judge, or other appropriate presiding judicial officer made or entered in writing, or on the record in a legal proceeding.

D. Data: All data collected, created, received, maintained, or disseminated by a government entity regardless of its physical form, storage media, or conditions of use, including, but not limited to, paper records and files, microfilm, computer media, or other processes.

E. Data Subject: The individual or person about whom the data is created or collected.

F. Designee: Any person designated by a responsible authority (a) to be in charge of individual files or systems containing government data and (b) to receive and comply with requests for government data. The responsibility authority may assign one or more designees. All duties outlined as duties of the responsible authority may be delegated to the designee.

G. Government Entity: A state agency, statewide system, or political subdivision.

H. Individual: A natural person. In the case of a minor or an individual adjudged mentally incompetent, "individual" includes a parent or guardian or an individual acting as a parent or guardian in the absence of a parent or guardian, except that the responsible authority shall withhold data from parents or guardians or individuals acting as parents or guardians in the absence of parents or guardians, upon request by the minor if the responsible authority determines that withholding the data would be in the best interest of the minor.

I. Informed Consent: The written consent that must be given by a data subject to allow disclosure of private data about the individual.

J. Person: Any individual, partnership, corporation, association, business trust, or legal representative of an organization.

K. Political Subdivision: Any county, statutory or home rule charter city, school district, special district, any town exercising powers under Minn. Stat. 368 and located in a metropolitan area, and any board, commission, district or authority created pursuant to law, local ordinance, or charter provision. It includes any nonprofit corporation which is a community action agency organized to qualify for public funds, or any nonprofit social service agency which performs services under contract to a government entity to the extent that the nonprofit social service agency or nonprofit corporation collects, disseminates, and uses data on individuals because of a contractual relationship with a government entity.

L. Representative of the Decedent: The personal representative of the estate of the decedent during the period of administration, or if no personal representative has been appointed, or after discharge, the surviving spouse, any child of the decedent, or, if there are not surviving spouse or children, the parents of the decedent.

M. Requestor: The individual, entity, or person requesting access and/or copies of the government data.

N. Responsible Authority-Counties: The HPH Administrator shall be the responsible authority of HPH. a statewide system, the responsible authority is the commissioner of any state department, or an

executive office designated by statute or executive order as responsible for such system.

O. Rules: "The Rules Governing the Enforcement of the Minnesota Government Data Practices Act." Minn. R., Chap. 1205.

P. State Agency: The state, the University of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district, or agency of the state.

Q. Statewide System: Any recordkeeping system in which government data is collected, stored, disseminated, and used by means of a system common to one or more state agencies or more than one of its political subdivisions or any combination of state agencies and political subdivisions.

R. Temporary Classification: An application by a state agency, statewide system, or political subdivision, pursuant to Minn. Stat. § 13.06 which has been approved by the Commissioner of Administration to classify government data not classified by state statute or federal law as either private or confidential for data on individuals, or nonpublic or protected nonpublic for data not on individuals.

S. Tennessen Warning: Those rights, as contained in Section IX.A, communicated to an individual asked to supply private or confidential data concerning himself or herself.

III. CLASSIFICATION OF GOVERNMENT DATA

For the purposes of these guidelines, government data is divided into four types; (a) data on individuals, which is classified as either public, private or confidential; (b) data not on individuals, which is classified as either public, nonpublic or protected nonpublic; (c) statistical or summary data derived from data on individuals in which individuals are not identified; and (d) data on decedents. These classifications, the criteria for classification, and the description of who has access are as set forth below.

A. Data on Individuals

a. **Public Data on Individuals**

i. **Definition:** All data on individuals is public, unless classified as private or confidential.

ii. **Data on Individuals is Public if:**

1) A statute or federal law requires or allows the collection of the data and does not classify the data as private or confidential.
2) An application for Temporary Classification for private or confidential data on individuals is disapproved by the Commissioner of Administration.
3) The data is summary or statistical data derived from data on individuals.
4) Private or confidential data becomes public in order to comply with either judicial or administrative rules pertaining to the conduct of legal action. (For example: Private or confidential data which is presented in court and made public by the court.)

iii. **Access:** All public data on individuals is accessible by any person regardless of their interest in that data.

b. **Private Data on Individuals**

i. **Definition**: Private data on individuals is data which is not accessible to the public, but is accessible to the individual subject of the data.

ii. **Tennessen Warning**: Except for law enforcement investigations, a Tennessen Warning must be given when private data is collected from the subjects of the data (Section VII.A. describes the Tennessen Warning.) A Tennessen Warning need not be given when private data is collected from someone other than the subject of the data.

iii. **Data on Individuals is Private if:**

1) A state statute or federal law expressly classifies the data as not accessible to the public, but accessible to the subject of the data.
2) A Temporary Classification of private has been approved by the Commissioner of Administration and has not expired.
3) If data is classified as both private and confidential by state or federal law, the data is private.

iv. **Access:** Private data on individuals is accessible to:

1) The individual subject of the data, or the representative as authorized in writing (if the subject is a minor, usually by the subject's parent or guardian).
2) Individuals, entities, or persons who have been given express written permission by the data subject.
3) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee.
4) Individuals, entities, or persons who used, stored, and disseminated government data collected prior to August 1, 1975, with the condition that use, storage, and dissemination was not accessible to the public, but accessible to the data subject.
5) Individuals, entities, or persons for which a state, local or federal law authorizes new use or new dissemination of the data.
6) Individuals, entities, or persons subsequent to the collection of the data and subsequent to the communication of the Tennessen Warning, when specifically approved by the Commissioner of Administration, as necessary to carry out a function assigned by law.
7) Pursuant to court order.
8) Individuals, entities, or persons as otherwise provided by law.

c. **Confidential Data on Individuals**

i. **Definition:** Data not made public by statute or federal law applicable to the data and are

inaccessible to the individual subject of those data.

ii. **Tennessen Warning:** Except for law enforcement investigations, a Tennessen Warning must be given when private data is collected from the subject of the data (Section VII.A. describes the Tennessen Warning.) A Tennessen Warning need not be given when private data is collected from someone other than the subject of the data.

iii. **Data on Individuals is Confidential if:**
   1) A state or federal statute expressly provides that: (a) the data shall not be available to either the public or to the data subject, or (b) the data shall not be available to anyone except those agencies which need the data for agency purposes.
   2) A Temporary Classification of confidential has been approved by the Commissioner of Administration and has not expired.

iv. **Access:** Confidential data on individuals is accessible to:
   1) Individuals, entities, or persons who are authorized by state, local or federal law to gain access.
   2) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee.
   3) Individuals, entities, or persons who used, stored, and disseminated government data collected prior to August 1, 1975, with the condition that use, storage, and dissemination was not accessible to the public, but accessible to the data subject.
   4) Individuals, entities, or persons for which a state, local or federal law authorizes new use or new dissemination of the data.
   5) Individuals, entities, or persons subsequent to the collection of the data and subsequent to the communication of the Tennessen Warning, when specifically approved by the Commissioner of Administration, as necessary, to carry out a function assigned by law.
   6) Pursuant to court order.
   7) Individuals, entities, or persons as otherwise provided for by law

B. Public, Nonpublic, or Protected Nonpublic Data Not on Individuals

a. **<u>Public Data Not on Individuals</u>**

i. **Definition:** Public data not on individuals means data not on individuals which is accessible to the public.

ii. **Data Not on Individuals is Public if:**
   1) A statute or federal law does not expressly classify the data as not public.
   2) An application for Temporary Classification for data as nonpublic or protected nonpublic is not approved by the Commissioner of Administration.
   3) A statute requires the data to be made available to the public.

iii. **Access:** Protected nonpublic data is accessible to:
   1) Personnel within Horizon Public Health whose wok assignment requires access as determined by the responsible authority or the designee;
   2) Individuals, entities, or persons authorized by statute or federal law to gain access;
   3) Pursuant to a court order; or
   4) Individuals, entities, or persons as otherwise provided by law.

b. **Nonpublic Data Not on Individuals**

i. **Definition:** Nonpublic data not on individuals means data that are not public but are accessible to the data subject, if any.

ii. **Data Not on Individuals is Nonpublic if:**
   1) A state statute or federal law classifies the data as not public but accessible to the data subject, if any.
   2) A Temporary Classification of data as nonpublic has been approved by the Commissioner of Administration

iii. **Access:** Nonpublic data not on individuals is accessible to:
   1) The data subject, if any.
   2) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee
   3) Entities or persons authorized by statute o federal statute to gain access.
   4) Pursuant to court order.
   5) Entities or persons as otherwise provided by law.

c. **Protected Nonpublic Data Not on Individuals**

i. **Definition:** Protected nonpublic data not on individuals means data that is not public and not accessible to the data subject, if any.

ii. **Data Not on Individuals is Protected Nonpublic if:**
   1) A state statute or federal law classifies the data as not accessible to the public and not accessible to the data subject.
   2) A Temporary Classification of government data as protected nonpublic has been approved by the Commissioner of Administration.

iii. **Access:** Protected nonpublic data not on individuals is accessible to:
   3) Personnel within the entity whose work assignment requires access as determined by the responsible authority or the designee.
   4) Entities or persons authorized by statute or federal statute to gain access.
   5) Pursuant to court order.
   6) Entities or persons as otherwise provided by law

C. Summary Data

i. **Definition**: Summary data means statistical records and reports derived from data on individuals, but in which the individuals are not identified and neither their identities nor other characteristics that could uniquely identify the individual is ascertainable.

ii. **Data is Summary Data if:**

1) All data elements that could link the data to a specific individual have been removed; AND

2) Any list of numbers or other data which could uniquely identify an individual is separated from the summary data and is not available to persons who gain access to or possess summary data.

iii. **Access:** Unless classified by a Temporary Classification, summary data is public and may be requested by and made available to any individual or person, including a government entity.

D. Data on Decedents

a. **<u>Private Data on Decedents</u>**

i. **Definition**: Upon death, private and confidential data on an individual shall become, respectively, private data on decedents and confidential data on decedents.

ii. **Access**

1) Access is available to the personal representative of the estate during the administration or if no personal representative, the surviving spouse, any child of the decedent, or if no spouse or children, to the parent of the decedent.
2) A trustee appointed in a wrongful death action also has access to the appropriate data on decedents concerning the data subject.

b. **<u>Confidential Data on Decedents</u>**

i. **Definition**: Confidential data on decedents means data which, prior to the death of the subject, was classified by statute, federal law, or temporary classification as confidential data.

ii. **Access:** Access to the data is the same as access to confidential data on individuals.

iii. The representative of the decedent may exercise all rights which are conferred by the Act on individuals who are subjects of the confidential data, in the case of confidential data on decedents.

c. Release of private data on a decedent or confidential data on a decedent may also be obtained from a court following the procedure outlined in the statute.

d. Private data on decedents and confidential data on decedents shall become public 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.

IV. HORIZON PUBLIC HEALTH DATA PRACTICES REQUESTS

A. Requests for Data on Individuals by the Data Subject

a. Upon request and when access or copies are authorized, the designee shall provide copies of the private or public data on an individual to the subject of the data or authorized representative. See Minn. R. 1205.0500 if data subject is a minor.

b. The designee shall comply immediately, if reasonably possible, or within 10 working days of the date of request, if immediate compliance is not reasonably possible.

c. After an individual has been shown the private data and informed of its meaning, the data need not be disclosed to that individual for six months, unless a dispute or action is pending (concerning accuracy of data) or additional data has been obtained about that individual.

d. A guide titled "Data Practices for Data Subjects" and a Request by Subject of Data form is available for the public and can be found here: ***www.horizonpublichealth.org***

e. The Request by Subject of Data form shall be completed for all requests by the public for government data which is classified as other than public.

B. Requests for Data – General

a. Upon request to the responsible authority or designee, an authorized person shall be permitted to inspect government data at reasonable times and places. If the party requests they shall be informed of the meaning of the data. If the data requested is public data, no form is necessary. Upon request and at the discretion of the staff member, public data may be disclosed over the telephone.

b. Regardless of where the data originates, if is in the position of Horizon Public Health, it is government data and subject to the Data Practices Act, including access provisions.

c. A guide titled "Data Practices for Members of the Public" and a Public Data Request form is available for the public and can be found here: *www.horizonph.org*

d. The Public Data Request form shall be completed for all requests by the public for government data which is classified as other than public.

C. Requests for Summary Data

a. Unless otherwise classified by a Temporary Classification, summary data derived from private or confidential data on individuals is public and the responsible authority or designee shall provide the summary data upon the written request of any individual or person.

b. Within ten (10) days of receipt of such request, the responsible authority or designee shall inform the requestor of the costs of preparing the summary data, if any.

c. The responsible authority or designee shall:

   i. Provide the summary data requested as soon as reasonably possible; OR

   ii. Provide a written statement to the requestor, giving a time schedule for preparing the requested data, including reasons for any delays; OR

   iii. Provide access to the requestor to the private or confidential data so that the requestor can compile the summary; OR

   iv. Provide a written statement to the requestor stating reasons why the requestor's access would compromise the private or confidential data.

d. A non-disclosure agreement (see Appendix B) is used to protect the confidentiality of government data when the requestor of the summary data prepares the summary by accessing private or confidential information on individuals. A non-disclosure agreement shall contain at least the following:

   i. A general description of the private or confidential data which is being used to prepare the summary data.
   ii. The purpose for which the summary data is being prepared.
   iii. A statement that the requestor understands that the requestor may be subject to the civil or criminal penalty provisions of the Act.
   iv. The signature of the requestor and the responsible authority, designee, or representative.

e. A non-disclosure agreement (see Appendix B) is used to protect the confidentiality of government data when the requestor of the summary data prepares the summary by accessing private or confidential information on individuals. A non-disclosure agreement shall contain at least the following:
   i. A general description of the private or confidential data which is being used to prepare the summary data.
   ii. The purpose for which the summary data is being prepared.
   iii. A statement that the requestor understands that the requestor may be subject to the civil or criminal penalty provisions of the Act.

iv. The signature of the requestor and the responsible authority, designee, or representative.

D. Requests for Government data by Other Government Agencies

a. A responsible authority shall allow another government entity access to data classified as private, confidential, nonpublic, or protected nonpublic only when the access is authorized or required by state or federal statute.

b. An agency that supplies government data under this section may require the requesting agency to pay the actual cost of supplying the data when the requested data is not provided in the normal course of business and not required by state or federal statute.

c. In most cases, data shall have the same classification in the hands of the agency receiving it as it had in the agency providing it, unless the classification is required to change to meet judicial or administrative requirements. When practical and necessary, the agency providing the requested information shall indicate the classification of the information.

d. When practical and necessary, the requesting agency not listed on the Tennessen Warning shall obtain the informed consent from the data subject(s) for data classified as private or confidential.

E. How Data Practices Applies to Contractual Licensing and Funding Relationship within Government Entities

a. Pursuant to Minn. Stat. § 13.05, Subd. 6, if a person receives not public data on individuals from a government entity because that person has a contract with that entity the person must administer the data in a manner that is consistent with the MGDPA.

b. Pursuant to Minn. Stat. § 13.05, Subd. 11, if a private person collects, receives, stores, uses, maintains or disseminates data because the person has a contract with a government entity to perform any of the entity's functions all of the data are subject to the requirements of the MGDPA and the contactor must comply with the MGDPA requirements. The contractor may be sued under § 13.08, civil remedies. The contract should clearly inform the contractor of these responsibilities.

c. Pursuant to Minn. Stat. § 13.02, Subd. 11, if the data is collected by a nonprofit social services entity that performs services under contract to a government entity and the data is collected and used because of that contract access to the data is regulated by the MGDPA.

d. If a third party is licensed by a government entity and the licensure is conditioned upon compliance with the MGDPA or if the party has another type of contact with the government entity, the party is subject to the MGDPA to the extent specified in the contract or the licensing agreement.

F. Data Request Forms

Data Request Forms: Forms for Data Subjects and Members of the Public are available in Agency offices and on the website at Data Requests. These forms are available in Agency offices and on the Agency website. The forms provide a record of the requestor identification information and the government data requested, as well as the action taken by the responsibility authority, or the designee, and any financial transaction which occurs. <u>These forms are to be completed for all requests by the public for government data.</u>

V. FEES FOR COPIES OF GOVERNMENT DATA

Pursuant to the Minnesota Government Data Practices Act and Horizon Public Health Community Health Board resolution and unless otherwise provided for by federal law, state statute or rule, fees for copies of government data shall be determined by HPH based on costs to provide such service. If the fee for fulfilling the request is greater than $5.00, pre-payment may be required.

1. **Copies Provided at No Charge**. When access is authorized, copies may be provided at no charge:

    i. When another government agency or responsible authority requires or requests the record/document copies as part of the administration and management of an authorized program and the copies are usually provided as part of the normal course of business.

    ii. When records, documents, brochures, pamphlets, books, reports, or other similar publications are produced for free distribution to the public. A charge may be assessed if an individual request exceeds normal distribution.

    iii. When the court orders the requesting party to proceed in forma pauperis.

2. **Copies Provided with Charge.** When access is authorized, copies shall be provided at the applicable rate in the following circumstances:

    i. Other government agencies or responsible authorities who require or request record documents or publication copies which are not usually provided or reproduced as part of the normal course of business

ii. Records, documents, brochures, pamphlets, books, reports, or other similar publications that are not normally provided or reproduced for distribution to the public.

iii. Public data on individuals and public data not on individuals, particularly when the requestor is not the subject of the data.

3. **Fees.** Copying fees shall be charged in accordance with the federal law and state statute or rule for those records, documents, and publications covered in Section B as set forth above. When copies are mailed, postage costs shall be added to the rates in the Fee Schedule. Fees shall be collected before releasing copies unless prior arrangements have been made.

VI. DUTIES OF THE RESPONSIBLE AUTHORITY OR DESIGNEE

1. **Data Inventory**

i. The responsible authority shall prepare an inventory containing the authority's name, title, address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the authority's government entity. Forms used to collect private and confidential data may be included in the inventory.

ii. The responsible authority shall update the inventory annually and make any changes necessary to maintain the accuracy of the inventory.

iii. The responsible authority shall supply the document to the Commissioner of Administration, State of Minnesota, if requested by the Commissioner.

2. **Procedures for Dissemination of Data**

i. The responsible authority shall ensure that each department establishes procedures to manage the dissemination of data. Collection, storage, use and dissemination of private and confidential data shall be limited to what is necessary of the administration and management of programs authorized or mandated by the state, local governmental body, or the federal government.

ii. Data cannot be collected, stored, used or disseminated for any purpose other than the purpose stated to the individual when the data was originally collected unless:

1. The data was collected prior to 1975, in which case the data can be used for the original purpose for which it was collected or for an additional purpose approved by the Commissioner of Administration.
2. There is specific authorization for the use in state, local or federal law.
3. The additional use has been approved by the Commissioner of Administration, as necessary, to carry out a function designated by law.
4. The individual data subject has given informed consent for the additional use of the data.

3. **Data Protection**

The responsible authority shall establish procedures to assure that all data on individuals is accurate, complete, and current for the purpose for which it was collected, and establish appropriate security safeguards for all records containing data on individuals.

4. **Assignment of Designee**

The responsible authority may assign one or more designees. The designee is the person in charge of individual files or systems containing government data and who receives and complies with requests for government data. Additionally, the designee shall implement the provisions of the Act, the rules, and these guidelines and procedures as directed by the responsible authority. All duties outlined as duties of the responsible authority may be delegated to the designee.

Responsible Authority: Horizon Public Health Administrator/designee

VII. RIGHTS OF DATA SUBJECTS

The Minnesota Government Data Practices Act establishes specific rights for *individuals* who are the subjects of government data, and establishes controls on how entities collect, store, use and release data about individuals. HPH's policy adheres to these regulations.

These rights include:

- The right to be given a notice (Tennessen Warning) when either private or confidential date about the subject are collected from the subject;
- The right to know whether a government entity maintains any data about the subject and how those data are classified;
- The right to inspect, at no charge, all public and private data about the subject;
- The right to have the content and meaning of public and private data explained to the subject;
- The right to have copies of public and private data about the subject at actual and reasonable cost;
- The right to have private or confidential data about the subject collected, stored, used or disclosed only in ways that are authorized by law and that are stated in the Tennessen warning notice; or in ways to which the subject as consented via an informed consent;
- The right not to have private or confidential data about the subject disclosed to the public unless authorized by law;
- The right to consent to the release of private data to anyone; and
- The right to be informed of these rights and how to exercise them within the entity that maintains the

data.

1. Tennessen Warning

The MGDPA guarantees certain rights to every individual from whom Horizon Public Health collects private or confidential data. Every department that collects private and confidential data from an individual concerning him/herself will, prior to collecting the data, inform the individual of his/her rights as a subject of data. The listing of rights is referred to as the Tennessen Warning. Once the proper notice has been given, Horizon Public Health may lawfully collect, store, use and disseminate

i. The Tennessen Warning is required and notice must be given whenever:

   1. The government *entity requests* the data; and

   2. The data are requested from an *individual*; and

   3. The data requested are *private or confidential*; and

   4. The data are *about the individual from* whom they are requesting.

ii. The Tennessen Warning is not required:

   1. When collecting public data on an individual;

   2. When private and confidential data is collected from someone other than the subject of the data, or that person supplies private or confidential data about the data subject without being asked for it;

   3. When an individual is asked to supply investigative data to a law enforcement officer (see Minn. Stat. § 13.04, Subd. 2).

   4. When an individual volunteers private or confidential information about himself or herself without being asked.

iii. The Tennessen Warning consists of the following information that must be communicated to the individual from whom private or confidential data concerning himself or herself is collected:[11]

   1. The purposes and intended use of the requested private or confidential data within the collecting statewide system or political subdivision or agency;

   2. Whether the individual may refuse or is legally required to supply the requested private or confidential data;

[1] Note: In accordance with the Federal Private Act of 1974, any federal, state, or local agency which requests an individual to disclose their social security number shall inform that an individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited and what uses will be made of it.

3. Any known consequences arising from an individual refusing to supply private or confidential data; and
4. The identity of other individuals, entities or persons authorized by state or federal law to receive the data.

5. Tennessen Warning may be either oral or written, however, a written format signed by the individual is preferred.

iv. Tennessen Warning for Minors

If private or confidential data is collected from a minor (under 18 years of age), additional notification is required. (See Notification to Minors, Section VIII.B.)

2. **Informed Consent for the Release of Data**

i. Private data on individuals may be used by and disseminated to any individual or person by the responsible authority, or the designee, if the individual subject or subjects of the data have given their informed consent.

ii. Private data may be used by and disseminated to any entity (e.g., political subdivision, government agency, etc.) if the individual subject or subjects have given their informed consent.

iii. All informed consents shall be in writing.

3. **When Informed Consent is NOT Required:**

i. For any lawful purpose which was communicated to the data subject on the Tennessen Warning at the time the data was collected,

ii. When a federal, state or local law authorizes access to the data after the Tennessen Warning was given, if required, or

iii. When the Commissioner of Administration, upon application, approves a new use or dissemination of the data and the new use and dissemination was not communicated to the data subject.

Informed consent for health insurance purposed must comply with Minn. Stat. § 13.05, unless otherwise pre-empted by the HIPPA Standards for Privacy of Individually Identifiable Health Information, code of Federal Regulations, title 45, section 164.

VIII. PARENTAL ACCESS TO DATA ON MINORS

1. **Access to a Minor's Data by Parents, Guardians or Acting Guardians**

i. A parent or guardian, or an individual acting as a parent or guardian in the absence of a parent or guardian, has access to all public government data on a minor data subject. Such person further has access to all private government data on a minor data subject, unless otherwise specifically

denied access by a state or federal law.

ii. Horizon Public Health will presume that a parent has authority to exercise rights of the minor inherent in the Act, unless the agency has been provided with evidence that there is a state law or court order governing such matters as divorce, separation, or custody, or a legally binding instrument that provides the contrary.

2. **Notification to Minors**

i. A minor has the right to request that the entity withhold private data about her/him from the parent or guardian. The entity may require that the request be in writing. A written request must include the reasons for withholding the data from the parents or guardian and must be signed by the minor.

ii. In making a determination to honor the request, the responsible authority must consider the following:

1. Whether the minor is of sufficient age and maturity to be able to explain the reason for and to understand the consequences of the request to deny access;
2. Whether the personal situation of the minor is such that denying the parental access may protect the minor from physical or emotional harm;
3. Whether there is reason to believe that the minor's reasons for denying access are reasonably accurate;
4. Whether the data concerns medical, dental, or other health services provided concerning the "Consent of Minors for Health Services" pursuant to Minn. Stat. §§ 144.335-144.337. However, this medical data may be released if failure to inform the parent would seriously jeopardize the health of the minor.
5.

IX. DATA SUBJECTS RIGHT TO APPEAL TO THE COMMISSIONER OF ADMINISTRATION IF ACCURACY AND/OR COMPLETELNESS OF DATA IS CHALLENGED

1. The subject has the right to take this step after both the subject and HPH have properly completed all the steps in the data challenge process. The subject may appeal only HPH's determination about the accuracy and/or completeness of the data.

2. The requirements for filing an appeal are set forth in Minnesota Rules Section 1205.1600.

X. CONSEQUENCES FOR NOT COMPLYING WITH THE MGDPA

1. Otter Tail Agency employees are to comply with Minn. Stat. §13.05, Subd. 5, and only access data that is private or confidential if their work assignment reasonably requires access to the data and it is only accessed for purposes specific to the work assignment. Additionally, pursuant to the Driver's Privacy Protection Act (DPPA), Driver and Vehicle Services (DVS) and the Bureau of Criminal Apprehension (BCA) databases are only to be used for official government-related and law-enforcement related purposes.

2. Pursuant to Minn. Stat. § 13.08, a government entity and employees may be sued for violating MGDPA.

3. Minn. Stat. § 13.085 provides an administrative process to compel compliance with MGDPA.

4. Minn. Stat. § 13.09 provides criminal penalties and disciplinary action as extreme as dismissal from public employment for anyone who willfully (knowingly) violates MGDPA.

XI. WHERE MORE INFORMATION CAN BE FOUND

1. Minnesota Statutes Chapter 13 is found on the website of the Revisor of Statutes at: www.leg.state.mn.us/leg/statutes.asp

2. Minnesota Rules, Chapter 1205, is found on the website of the Revisor of Statutes at: www.revisor.leg.state.mn.us/arule/1205

3. Responsible Authority Ann Stehn, Horizon Public Health, at 320-763-6018 or info@horizonph.org.

XII. OTHER PROTECTED DATA

1. The Driver's Privacy Protection Act (DPPA) prevents the release and use of certain personal information from State motor vehicle records. It is permissible for an employee to access this information for work purposes. The DPPA establishes criminal fines for non-compliance and establishes a civil cause of action for drivers against those who unlawfully obtain personal information. See also 18 U.S. Code § 2721.
2. The Health Insurance Portability and Accountability Act (HIPAA) provides data privacy and security provisions for safeguarding medical information. More information can be found at the U.S. Department of Health and Human Services

APPENDIX A

THE NOTICE OF RIGHTS TENNESSEN WARNING
Minnesota Statutes § 13.04, Subdivision 2

- Notice must be given when an individual is asked to supply private or confidential data concerning self.

- Statements must be included from the individual that inform the individual the following:

- Why the data is being collected and how the entity intends to use the data;
    - Whether the individual may refuse or is legally required to supply the data;
    - Any consequences to the individual either supplying or refusing to supply the data; and
    - The identity of other persons or entities authorized by law to receive the data.

- Giving the notice allows HPH to obtain private or confidential data on individuals that may be collected, stored, and used as described in the notice without liability to the entity.

- Consequences of <u>not</u> giving the notice are that private or confidential data on individuals cannot be collected, stored, used or released for any purposes other than those stated in the notice unless:
    - The individual subject of the data gives informed consent;
    - The Commissioner of Administration gives approval;
    - A state or federal law subsequently authorizes o requires the new use or release; or
    - A Court order is issued to authorize release.

Appendix A (cont.)
"NOTICE OF RIGHTS"
SAMPLE FORMAT FOR TENNESSEN WARNING

The Data Practices Act requires HPH to inform you of your rights as they pertain to private data collected from you and about you. Some of the personal data we collect from you is private data. Access to this data is available only to you, the agency collecting the data, or other statutorily authorized agencies unless you or a court authorizes its release. This warning is given in accordance with Minnesota Statute § 13.04, Subd. 2.

The following must be completed:

The Data Practices Act requires that you be advised the following data that you are asked to provide is considered private data:

The purpose and intended use of the requested data is:

Authorized persons or agencies with whom this data may be shared include:

Furnishing the above data is voluntary, but refusal to supply the requested data will mean:

_____
Name

_____
Date

APPENDIX B
Non-Disclosure Agreement

1. General Description of the private or confidential data which is being used to prepare summary data:

2. Purpose for which summary data is being prepared:

3. I,_____, representing _____have requested the data described above and for the purposes stated and fully understand that I may be subject to the civil or criminal penalty provision of the Minnesota Data Practices Act in the event that the private or confidential data is disclosed.

Minn. Stat. §13.09: Any person who willfully violates the provisions of Minnesota Statutes Chapter 13, or any rules adopted or regulation promulgated thereunder is guilty of a misdemeanor. Any willful violation of Minnesota Statutes Chapter 13 by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.

_____ _____
Requestor of Data Date

_____ _____
Responsible Authority/Designee Date