

**MINNESOTA PUBLIC UTILITIES
COMMISSION**

**PUBLIC ACCESS TO GOVERNMENT DATA
AND
RIGHTS OF SUBJECTS OF DATA**

2006

Based on the Model Policy prepared by:

Minnesota Department of Administration
Information Policy Analysis Division
July, 2000

The Model Policy on which this document is based has been prepared by:

Minnesota Department of Administration
Information Policy Analysis Division
201 Administration Building
50 Sherburne Avenue
St. Paul, MN 55155]

Copyright 2000 Minnesota Department of Administration

The Minnesota Department of Administration does not discriminate on the basis of race, creed, color, sex, sexual orientation, national origin, age, marital status, disability, religion, reliance on public assistance or political opinions or affiliations in employment or the provisions of services. This document can be made available in alternative formats, such as large print, Braille or audio tape, by calling (651) 296.6733 or (800) 657.3721/Voice, or by looking at our Web site at: www.ipad.state.mn.us. For TTY communication, contact the Minnesota Relay Service at (800) 627.3529 and ask them to place a call to (651)296. 6733.

TABLE OF CONTENTS

| | |
|--|-----------|
| Section I. Introduction | 5 |
| • Why was this model written?..... | 5 |
| • What is the purpose of this model?..... | 5 |
| • What is the scope of this model? | 5 |
| • Who should use this model? | 6 |
| • How is the model organized and how may it be used?..... | 6 |
| • Why is the model not structured like a formal policy and procedure document? | 7 |
| • What meanings have been assigned to certain terms used in this model?..... | 7 |
| Section II. The MGDPA: A Summary of Provisions..... | 9 |
| • What is the Minnesota Government Data Practices Act?..... | 9 |
| • What are government data? | 9 |
| • Who must comply with the MGDPA?..... | 9 |
| • What is the classification system and how does it regulate access to data? | 10 |
| • What are the categories in the data classification system? | 10 |
| • What are the classifications within each of these three categories? | 11 |
| • How does one know how data are classified? | 12 |
| • How else does the MGDPA regulate data handling practices? | 12 |
| • What is the role of the Commissioner of Administration? | 13 |
| • What are the consequences for not complying with the MGDPA?..... | 13 |
| • Where can more information about the MGDPA be found? | 13 |
| • Documents: | |
| A BRIEF OVERVIEW OF THE MINNESOTA GOVERNMENT DATA PRACTICES ACT | 15 |
| THE MINNESOTA GOVERNMENT DATA PRACTICES ACT: DEFINITIONS AND CLASSIFICATIONS OF DATA | 17 |
| MINNESOTA GOVERNMENT DATA PRACTICES ACT: COMPLIANCE CHECKLIST | 19 |
| Section III. Duties of the Responsible Authority: | |
| Access to Government Data by Members of the Public | 23 |
| • What is the most basic requirement for properly responding to a data practices request?..... | 23 |
| • Are there other requirements relating to access to government data by the public? | 23 |
| • Who can make a data request?..... | 23 |
| • To whom must a data request be made? | 23 |
| • What kinds of data may a person request?..... | 24 |
| • Must a data request be made in writing? | 24 |
| • May an entity permit standing requests for data? | 24 |
| • Must a government entity respond to a data request?..... | 24 |
| • What kind of response must the entity make and how soon must it respond? | 24 |
| • How does an entity determine the appropriate response to a data request? | 24 |
| • What is the appropriate response if the requested data are not public? | 25 |
| • What is the appropriate response if the data are public? | 25 |
| • What limits may an entity place upon access to the requested data?..... | 25 |

| | |
|---|----|
| • What are the entity’s obligations if asked to explain the data provided?..... | 25 |
| • May an entity refuse to provide copies of public data? | 25 |
| • May an entity assess a fee for separating public from not public data? | 25 |
| • May an entity assess a fee for inspection of public data?..... | 26 |
| • May an entity assess a fee for providing copies of public data?..... | 26 |
| • May an entity assess an additional fee for providing copies of data that have commercial value? | 26 |
| • What special requirements apply to requests for summary data?..... | 27 |
| • Document: FEES FOR PROVIDING COPIES OF PUBLIC DATA | 29 |

Section IV. Duties of the Responsible Authority:

The Rights of Subjects of Government Data31

An important note about who may exercise the rights of the individual32

Actions at the point of data collection33

| | |
|--|----|
| • What controls are placed on the collection and storage of data on individuals? | 33 |
| • What actions must an entity take before collecting and storing data on individuals? | 33 |
| • What is a Tennessee warning notice?..... | 33 |
| • What must be included in the notice?..... | 33 |
| • When must the Tennessee warning notice be given? | 33 |
| • When is a Tennessee warning notice not required?..... | 34 |
| • How does an entity decide what to include in a Tennessee warning notice?..... | 34 |
| • How does one know that a notice is complete? | 34 |
| • What are some practical suggestions for drafting a Tennessee warning notice? | 34 |
| • Does a Tennessee warning notice have to be given in writing?..... | 35 |
| • What authority does the entity have when it has given the notice? | 35 |
| • What are the consequences of not giving the notice?..... | 35 |
| • Does this mean that the data never can be stored if a Tennessee warning notice was not given?..... | 35 |

Actions when data are used or released by the entity.....35

| | |
|--|----|
| • What controls are placed on the use and dissemination of data on individuals? | 35 |
| • What actions must an entity take before using or releasing private or confidential data on individuals? | 36 |
| • What authority does the entity have after giving a proper Tennessee warning notice? | 36 |
| • Can the entity use or release private or confidential data if it has not given a proper notice? | 36 |
| • Does this mean that the data never can be stored, used or released if a Tennessee warning notice was not given?..... | 36 |
| • Informed consent | |
| • Subsequent law | |
| • Old data | |
| • Special circumstances | |

Actions relating to the subject’s right to access data about herself or himself37

- The data subject has the right to ask and be told whether the entity maintains data about her/him, and whether those data are classified as public, private or confidential.37
- The data subject has the right to see all public and private data about her/himself.37
- Under certain circumstances, data about a minor data subject may be withheld from a parent or guardian.38
- The entity may not charge a fee for letting the subject see data about her/himself.39
- The subject has the right to be informed of the content and meaning of public and private data about her/himself upon request.39
- The subject has the right to get copies of all public and private data about her/himself. .39
- The entity may charge a fee for providing a data subject with copies of public and/or private data about her/himself.40

Actions relating to the right of the data subject to challenge the accuracy and/or completeness of public and private data about her/himself.....40

- The data subject has the right to challenge the accuracy and/or completeness of public and private data about her/himself.....40
- The data subject has the right to include a statement of disagreement with the disputed data.41
- If an entity determines that challenged data are accurate and/or complete, and the data subject disagrees with that determination, the subject has the right to appeal the entity’s determination to the Commissioner of Administration.41

Documents:

HOW TO DETERMINE WHETHER A GOVERNMENT ENTITY MAY LAWFULLY COLLECT, STORE, USE AND RELEASE DATA ON INDIVIDUALS43

HOW THE MINNESOTA GOVERNMENT DATA PRACTICES ACT CONTROLS ACCESS TO PRIVATE DATA ON INDIVIDUALS45

HOW THE MINNESOTA GOVERNMENT DATA PRACTICES ACT CONTROLS ACCESS TO CONFIDENTIAL DATA ON INDIVIDUALS47

THE TENNESSEN WARNING NOTICE49

MODEL CONSENT FOR THE RELEASE OF GOVERNMENT DATA51

CHALLENGING THE ACCURACY AND/OR COMPLETENESS OF DATA THAT GOVERNMENT ENTITIES KEEP ABOUT YOU.....57

Section V. Your Rights as a Member of the Public to Access Government Data61

- The law says that all the data we have are public (can be seen by anybody) unless there is a state or federal law that classifies the data as not public61
- You have the right to look at all public data that we keep.....61
- We don’t have to give you data that we don’t keep62
- We may not have to give you public data in the form you want62
- We cannot charge you a fee for looking at public data.....62
- You have the right to have public data explained in a way you understand.....62
- You have the right to have copies of the public data we keep.....62
- We have the right to charge you a reasonable fee for providing copies63
- You have the right to know why you can’t see or get copies of data that are not public...63
- You have the right to see and have copies of summary data63

| | |
|--|-----------|
| Section VI. Your Rights as the Subject of Government Data | 65 |
| • An important note about who may exercise your rights | 65 |
| • If you are a minor | |
| • If you have been appointed as the legal guardian for someone | |
| • The law controls how we collect, keep, use and release data about you | 65 |
| • The law says we have to give you a notice when we ask you to give us data about yourself. | 65 |
| • The notice puts limits on what we can do with the data we keep about you. | 66 |
| • If we need to use or release data about you in a new way, we need your permission | 67 |
| • You have the right to know if we keep data about you | 68 |
| • You have the right to see data we keep about you..... | 68 |
| • We can't charge you a fee for looking at data about yourself..... | 69 |
| • You have the right to have public and private data about you explained to you..... | 69 |
| • You have the right to have copies of data about yourself..... | 69 |
| • We have the right to charge a fee for making the copies | 69 |
| • You have the right to know why you can't see or get copies of data we keep about you | 69 |
| • You have the right to challenge the accuracy and/or completeness of data about you ... | 69 |
| • You have the right to include a statement with inaccurate and/or incomplete data | 70 |
| • You can appeal our decision about your data challenge..... | 70 |

SECTION I INTRODUCTION

Why was this model written?

In Chapter 250, Section 41 of the 1999 Minnesota Session Laws, the Legislature directed the Commissioner of Administration to A...prepare model policies and procedures to assist government entities in complying with the requirements of [Chapter 13, the Minnesota Government Data Practices Act] that relate to public access to government data and rights of subjects of data.

The Legislature further directed that the model be prepared in consultation with affected government entities and that the completed model be offered to these entities to either adopt or reject. In response to these directives, the Information Policy Analysis Division of the Minnesota Department of Administration prepared this model policy.

What is the purpose of this model?

The Minnesota Government Data Practices Act (MGDPA) sets out certain requirements relating to the right of the public to access government data and the rights of individuals who are the subjects of government data. These are key and fundamental components of the MGDPA, and are the two components which provoke the greatest number of questions.

The purpose of the model is to explain, in a practical way, what the MGDPA requires of each government entity as it establishes its own specific data practices policies and procedures. Portions also are intended to be useful to anyone seeking access to public data and to individuals who are the subjects of government data.

What is the scope of this model?

This model provides 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*. Although the MGDPA establishes other requirements, they are not discussed here. For further information on these other requirements, see Chapter 13, itself, and the Rules previously adopted by the Department of Administration, Minnesota Rules, Chapter 1205.

The public access requirements discussed in this model are:

- The presumption that all government data are public unless classified as not public by state statute or federal law;
- The right of anyone to know what kinds of data are collected by the government entity and how those data are classified;
- The right of anyone to inspect, at no charge, all public government data at reasonable times and places;
- The right of anyone to have public data explained in an understandable way;
- The right of anyone to have copies of public government data at a reasonable cost;

- The right of anyone to an appropriate and prompt response from the government entity when exercising these rights; and
- The right of anyone to be informed of the authority by which an entity can deny access to government data.

(See Minnesota Statutes section 13.03, subdivisions 1- 3.)

The rights of data subjects addressed in this model are:

- 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 be given a notice (Tennessee warning) when either private or confidential data about the subject are collected from the subject;
- 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 Tennessee warning notice; in ways to which the subject has consented via an informed consent; or in ways that are authorized by law after the data have been collected;
- 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.

(See Minnesota Statutes section 13.04; section 13.05, subdivisions 3 and 4; and section 13.05, subdivision 8.)

Who should use this model?

The model is designed to be used by:

- the responsible authority, the data practices compliance official, and other employees in state agencies, counties, cities, school districts and other political subdivisions;
- local government officials;
- members of the public who are seeking access to government data; and
- individuals who are the subjects of government data.

How is the model organized and how may it be used?

The model is composed of the following sections, each of which includes documents referenced within:

Section II provides a *summary of key elements* of the MGDPA which are relevant to the model. Information in this section may be used by entity staff, and may be provided to the public and to individual data subjects.

Section III is *addressed to the responsible authority* for each government entity, and describes what is required of the entity in order to comply with requirements relating to *the right of the public to access government data*. This section is intended to guide the responsible authority in

establishing the specific procedures required of each entity by the MGDPA. The entity may provide any of the documents in this section to the public in order to achieve compliance with the public notice requirements of Minnesota Statutes section 13.03, subdivision 2(b).

Section IV describes what is required of each government entity in order to comply with requirements relating to *the rights of subjects of data*. Also *addressed to the responsible authority*, this section is intended to guide the entity in establishing the specific procedures required of each entity by the MGDPA. The entity may provide any of the documents in this section to the data subject in order to comply with the requirement that the subject be informed of her/his rights and how to exercise them within the entity. (Minnesota Statutes section 13.05, subdivision 8.)

Section V is written from the perspective of a government entity. It is *addressed to members of the public* to guide them in exercising their right to access government data. Each government entity may tailor the contents of Section V to its specific needs and provide it to the public in order to comply with the public notice requirements of Minnesota Statutes section 13.03, subdivision 2(b).

Section VI also is written from the perspective of a government entity. It is *addressed to the subjects of government data* to guide them in exercising their rights under the MGDPA. Each government entity may tailor the contents of this section to its specific needs and provide it to data subjects to comply with the requirements of Minnesota Statutes section 13.05, subdivision 8.

Why is the model not structured as a formal policy and procedure manual?

The MGDPA requires each of the over 3000 state and local government entities in Minnesota to establish data practices policies and procedures. The specific procedures for any given entity necessarily will vary by level of government and according to numerous other factors, including entity function, size, and structure.

What meanings have been assigned to certain terms used in this model?

The term, *data*, when used in this model, means government data, as discussed in Section II.

Entity refers to a state agency or political subdivision and includes any organization that is subject to the MGDPA.

MGDPA is the Minnesota Government Data Practices Act, Chapter 13 of Minnesota Statutes.

Person refers to any member of the public, and includes individuals, members of the media, corporations, non-governmental organizations, etc.

Subject means a data subject; an individual who is the subject of government data.

SECTION II

THE MGDPA: A SUMMARY OF PROVISIONS

What is the Minnesota Government Data Practices Act?

The Minnesota Government Data Practices Act (MGDPA), which is Chapter 13 of Minnesota Statutes, is a state law that controls how government data are collected, created, stored (maintained), used and released (disseminated). See A BRIEF OVERVIEW OF THE MINNESOTA GOVERNMENT DATA PRACTICES ACT at the end of this section.

What are government data?

Government data are all data kept in any recorded form by government entities in the executive branch of government in Minnesota. As long as data are recorded in some way by a government entity, they are government data, no matter what physical form they are in, or how they are 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 do not include mental impressions.

It is important to remember that government data are regulated at the level of individual items or elements of data, so that any given document, record or file contains many data elements.

Who must comply with the MGDPA?

The law applies to *state agencies* in Minnesota. State-level entities include the University of Minnesota and state-level offices, departments, commissions, officers, bureaus, divisions, boards, authorities, districts and agencies.

The MGDPA applies to *political subdivisions*, including counties, cities, school districts, special districts, boards, commissions, districts and authorities created by law, local ordinance or charter provision. Although townships are political subdivisions, *the MGDPA does not apply to townships*.

Statewide systems are subject to the MGDPA. A statewide system is a record keeping or data administering system that is established by federal law, state statute, administrative decision or agreement, or joint powers agreement, and that is common to any combination of state agencies and/or political subdivisions.

Community action agencies organized pursuant to the Economic Opportunity Act of 1964 also are subject to the MGDPA.

Persons or entities licensed or funded by, or under contract to, a government entity are subject to the MGDPA to the extent specified in the licensing, contract or funding agreement. Specifically:

- Pursuant to Minnesota Statutes section 13.05, subdivision 6, if a person receives 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.
- Pursuant to Minnesota Statutes section 13.05, subdivision 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 contractor must comply with MGDPA requirements. A contractor who fails to comply may be sued under section 13.08, civil remedies. The contract must clearly inform the contractor of these responsibilities.
- Pursuant to Minnesota Statutes section 13.02, subdivision 11, if the data are collected by a nonprofit social services entity which performs services under contract to a government entity, and the data are collected and used because of that contract, access to the data is regulated by the MGDPA.
- 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 contract with a government entity, the party is subject to the MGDPA to the extent specified in the contract or the licensing agreement.
- Pursuant to Minnesota Statutes section 13.46, persons contracting with portions of the welfare system may be subject to the MGDPA because of the contract.

The Courts and the Legislature are not subject to the MGDPA.

What is the data classification system and how does it regulate access to data?

One important way in which the MGDPA regulates access to government data is by establishing a system of data classifications that define, in general terms, who is legally authorized to access the data. The classification system consists of three categories of data. Each data category contains three data classifications. Every data element must fall into one of the nine resulting classifications. See, THE MINNESOTA GOVERNMENT DATA PRACTICES ACT: DEFINITIONS AND CLASSIFICATIONS OF DATA, at the end of this section.

What are the *categories* in the data classification system?

At the most basic level, the system establishes three categories of government data:

- **Data on individuals** are any data which identify an individual (a living human being) or from which an individual can be identified.
- **Data *not* on individuals** are data that do not identify individuals. They include data about legally created persons such as business entities, as well as administrative, policy and financial information maintained by government entities. Data not on individuals also include:
 - Private or confidential data which have been stripped of any data that would identify an individual;
 - Data about an individual that are collected or created *after* that individual's death; and

- Summary data, which are private or confidential data which have been stripped of any data that would identify an individual, and which are used to produce statistical records or reports. For information on requirements relating to summary data, see Minnesota Statutes section 13.02, subdivision 19 and section 13.05, subdivision 7; and Minnesota Rules, part 1205.0700.
- **Data on decedents** are data about a deceased individual which were created or collected *before the individual's death*.

What are the data *classifications* within each of these three categories?

Within each of these three categories, the MGDPA establishes three data classifications. Each classification defines who is legally authorized to access data classified in that way.

*One of the classifications in all three categories is **public data**.* Government entities must provide public data to anyone upon request, regardless of who is requesting the data or why.

*Data in the other classifications in each category are **not public**.*

Not public classifications for **data on individuals** are as follows.

- **Private data** on individuals are, as a general rule, accessible only by the data subject (and, if the subject is a minor, by the subject's parent or guardian); by entity staff whose work assignments reasonably require access; by agencies and persons that are authorized by law to access the data; and by anyone with the consent of the data subject. See Sections IV and VI for detailed information about who may access private data on individuals.
- **Confidential data** on individuals generally are accessible only by authorized staff of the entity which maintains the data and by agencies and persons who are authorized by law to access the data. See Sections IV and VI for detailed information about who may access confidential data on individuals.

Not public classifications for **data not on individuals** are as follows.

- **Nonpublic** data not on individuals are not accessible to the public and are accessible to the data subject, if any. Although the MGDPA is silent on this point, it is reasonable to conclude that access to the data should be limited to entities or persons who have the legal authority to do so, and to entity staff on a need-to-know basis. It also is reasonable to conclude that a representative of the organization which is the subject of the data may access the nonpublic data and may consent to its release.
- **Protected nonpublic** data not on individuals are not available either to the public or to the subject of the data. Again, though not addressed by the MGDPA, it is reasonable to conclude that protected nonpublic data are accessible to entities or persons who are authorized by law to access the data, and to entity staff whose work assignments reasonable require access, but are not accessible to the data subject.

Not public classifications for **data on decedents** are as follows.

- **Private** data on decedents are data which, before the death of the data subject, were classified as private data on individuals. Access to private data on decedents is the same as access to private data on individuals. Additionally, the personal representative of the estate may access the data if the estate is in probate or, if not in probate, the data are accessible to the

surviving spouse or, if there is no surviving spouse, to the decedent's child or children. If there are no children, the decedent's parents may access the data. The MGDPA refers to the personal representative and the survivors of the decedent as the representative of the decedent.

- **Confidential** data on decedents are data, which before the death of the data subject, were classified as confidential data on individuals. Access to the data is the same as access to confidential data on individuals.

Access to data on decedents generally is the same as access to data on individuals. Upon the death of the individual data subject, the rights of the data subject transfer to the representative of the decedent. See Sections IV and VI for information about the rights of data subjects.

How does one know how data are classified?

The MGDPA classifies all government data as public unless a specific state statute or federal law classifies the data as not public. Government entities must determine what types of data they maintain and what data classifications apply to the data. If no statute or federal law can be identified that classifies the data as not public, the data are presumed to be public and available to anyone upon request.

The MGDPA itself classifies many types of government data. (See sections 13.30 through 13.90.) The last section of this law, section 13.99, lists other Minnesota Statutes that classify government data as not public, or that place restrictions on access to government data.

How else does the MGDPA regulate data handling practices?

In addition to classifying data, the MGDPA establishes important *rights for individuals who are the subjects of government data*. Many of these rights are established at Minnesota Statutes section 13.04 and are discussed more fully in Sections IV and VI of this manual.

The MGDPA does not establish comparable rights for businesses and other organizations which are the subjects of data not on individuals.

The MGDPA also imposes significant *duties on government entities*, many of which are established by Minnesota Statutes section 13.05. These duties, including the requirements relating to public access and the rights of data subjects discussed in this model, are summarized in the document, MINNESOTA GOVERNMENT DATA PRACTICES ACT: COMPLIANCE CHECKLIST at the end of this section. One requirement is that each government entity appoint a *responsible authority* to ensure compliance with the MGDPA. The duties of the entity are assigned to its responsible authority.

In the 2000 Legislative Session, section 13.05 was amended to require all government entities to appoint a *data practices compliance official* to whom questions or concerns about data practices problems may be addressed. The responsible authority may be the data practices compliance official. The official must be appointed by December 1, 2000.

What is the role of the Commissioner of Administration?

Pursuant to section 13.05, subdivision 4, the Commissioner of the Minnesota Department of Administration is given the authority to approve new uses and dissemination of private and confidential data on individuals.

Section 13.06 of the MGDPA gives to the Commissioner certain powers with regard to approving temporary classifications of data.

Section 13.072 of the MGDPA gives the Commissioner authority to issue advisory opinions concerning the rights of data subjects and the classification of government data. Commissioner's opinions may be found on the World Wide Web at: www.ipad.state.mn.us

Section 13.073 of the MGDPA authorizes the Commissioner to establish a program for training state and local government entities and officials on information policy issues.

What are the consequences for not complying with the MGDPA?

Pursuant to section 13.08 of the MGDPA, a government entity may be sued for violating any of the Act's provisions.

Section 13.09 provides criminal penalties, and disciplinary action as extreme as dismissal from public employment, for anyone who willfully (knowingly) violates a provision of the MGDPA.

Where can more information about the MGDPA be found?

The following sources may provide helpful information about the MGDPA and other data practices laws. It is important to note, however, that *only the legal advisor for an entity has the authority and responsibility to provide specific legal advice about the provisions of the MGDPA, and other laws, as they relate to that entity.*

Local government associations -- such as the Association of Minnesota Counties, the Minnesota County Insurance Trust, the League of Minnesota Cities, the Minnesota School Boards Association, the Minnesota Association of County Officials, and the Minnesota Police and Peace Officers Association -- may be consulted for information specific to matters within their jurisdiction.

Additionally, assistance with data practices issues is available from:

Information Policy Analysis Division (IPAD)
Minnesota Department of Administration
305A Centennial Building, 658 Cedar Street
St. Paul, MN 55155
Voice: 651.296.6733 or 1.800.657.3721
Fax: 651.205.4219
www.ipad.state.mn.us

Opinions issued by the Commissioner of Administration, pursuant to Minnesota Statutes section 13.072, are available on the IPAD Web site. Copies of individual opinions, an opinion summary, and an index to Commissioner's Opinions are available from IPAD upon request.

Minnesota Statutes Chapter 13 (the MGDPA) may be found on the Web site of the Revisor of Statutes at: <http://www.revisor.leg.state.mn.us/revisor.html>.

Minnesota Rules, Chapter 1205, the Rules Governing Data Practices, promulgated by the Minnesota Department of Administration, also may be found on the Web site of the Revisor of Statutes at: <http://www.revisor.leg.state.mn.us/revisor.html>.

A discussion of the history and operation of the MGDPA can be found in the following law review articles:

Data Privacy: Everything You Wanted to Know About the Minnesota Government Data Practices Act -- From A to Z, by Donald A. Gemberling and Gary A. Weissman, in the *William Mitchell Law Review*, Volume 8, Number 3 (1982).

Data Practices at the Cusp of the Millennium, by Donald A. Gemberling and Gary A. Weissman, in the *William Mitchell Law Review*, Volume 22, Number 3 (1996).

The Minnesota Government Data Practices Act: A Practitioner's Guide and Observations on Access to Government Information, by Margaret Westin, in the *William Mitchell Law Review*, Volume 22, Number 3 (1996).

A Brief Overview of the Minnesota Government Data Practices Act

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

Briefly, the Act regulates:

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

Almost all government data are 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. This classification system determines how government data are handled (see chart, below).

| Data on Individuals | Meaning of Classification | Data not 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 |

Information Policy Analysis Division, Department of Administration
 305A Centennial Building, 658 Cedar Street
 St. Paul, Minnesota 55155
 Voice: 651.296.6733 or 1.800.657.3721 Fax: 651.205.4219
 www.ipad.state.mn.us
 April 2000

**THE MINNESOTA GOVERNMENT DATA PRACTICES ACT:
DEFINITIONS AND CLASSIFICATIONS OF DATA**

The Minnesota Government Data Practices Act (MGDPA) establishes a system of data classifications that define, in general terms, who is legally authorized to access government data. This classification system is constructed from the definitions provided in Minnesota Statutes section 13.02. See also Minnesota Rules part 1205.0200.

| GOVERNMENT DATA All data kept in any recorded form, regardless of physical form, storage media, or conditions of use <small>MS §13.02, SUBDIVISION 7</small> | | |
|--|--|---|
| DATA ON INDIVIDUALS* <small>MS §13.02, SUBDIVISION 5</small> | DATA ON DECEDENTS <small>MS §13.10, SUBDIVISION 1</small> | DATA NOT ON INDIVIDUALS * <small>MS §13.02, SUBDIVISION 4</small> |
| PUBLIC Accessible to anyone for any reason <small>MS §13.02, SUBDIVISION 15</small> | PUBLIC Accessible to anyone for any reason <small>MS §13.02, SUBDIVISION 15</small> | PUBLIC Accessible to anyone for any reason <small>MS §13.02, SUBDIVISION 14</small> |
| PRIVATE Accessible to the data subject; Not accessible to the public <small>MS §13.02, SUBDIVISION 12</small> | PRIVATE ** Accessible to the representative of the decedent; Not accessible to the public <small>MS §13.10, SUBDIVISION 1B.</small> | NONPUBLIC Accessible to the subject of the data, if any; Not accessible to the public <small>MS §13.02, SUBDIVISION 9</small> |
| CONFIDENTIAL Not accessible to the data subject; Not accessible to the public <small>MS §13.02, SUBDIVISION 3</small> | CONFIDENTIAL** Not accessible to the representative of the decedent; Not accessible to the public <small>MS §13.10, SUBDIVISION 1A</small> | PROTECTED NONPUBLIC Not accessible to the data subject; Not accessible to the public <small>MS §13.02, SUBDIVISION 13</small> |

* Individual is defined at MS §13.02, subdivision 8. Individual means a living human being. It does not mean any type of entity created by law, such as a corporation.

** Private and confidential data on decedents become public data ten years after the death of the data subject *and* 30 years after the creation of the data.

**MINNESOTA GOVERNMENT DATA PRACTICES ACT:
COMPLIANCE CHECKLIST**

The Minnesota Government Data Practices Act (MGDPA), its accompanying rules, and related statutes impose specific obligations upon government entities to comply with the procedural requirements of the statute. This document summarizes these obligations.

The MGDPA is Chapter 13 of Minnesota Statutes. The Rules implementing the MGDPA are found in Minnesota Rules, Chapter 1205.

| MINNESOTA GOVERNMENT DATA PRACTICES ACT: COMPLIANCE CHECKLIST | | | |
|---|----------------------|--|--|
| Authority | Topic | Specific Obligation | Purpose |
| 1 MS §13.03, subd. 2; MN Rules 1205.0300 | Customer service | Establish procedures to ensure that officials respond promptly to requests for government data. Required in written form by January 1, 2001. | Facilitate public access; Hold entity accountable |
| 2 MS §13.05, subd. 8 | Access procedures | Prepare a public document setting forth the rights of data subjects and procedures for subjects to access public and private data about themselves | Inform citizens of their rights as subjects of government data, and explain how to exercise those rights |
| 3 MS §13.05, subd. 5(1); MN Rules 1205.1500 | Data quality | Establish procedures to ensure that data on individuals are accurate, complete and current | Protect against the use of erroneous data in making decisions that affect individuals |
| 4 MS §13.05, subd. 5(2) | Data security | Establish procedures to ensure security safeguards for data on individuals | Protect individual privacy; Prevent alteration of data |
| 5 MS §13.05, subd. 1; MN Rules 1205.1500, subpart 3 | Inventory of Records | Create and annually update an inventory of records containing data on individuals, including data collection forms | Create central repository of data classifications; Give notice of the data maintained by entity |

| MINNESOTA GOVERNMENT DATA PRACTICES ACT: COMPLIANCE CHECKLIST | | | |
|---|---|--|---|
| Authority | Topic | Specific Obligation | Purpose |
| 7 MS §13.05, subd. 11 | Contract provisions | When preparing contracts by which a private sector contractor performs government functions, insert provisions that clearly oblige the contractor to comply with MGDPA as if it were a government entity | Extend protection into the private sector where public sector performs government duties; Prevent government entities from concealing data in the private sector |
| 8 MS §13.05, subd. 7; MN Rules 1205.0700, subpart 3 | Summary data | Prepare summary data upon the written request of any person; establish procedures for gaining access to summary data | Provide reasonable access to data for research purposes while protecting individual identities. |
| 9 MS §13.05, subd. 9, 10 | Dissemination of not public data to other governmental entities without authority | An entity may not share not public data with another entity unless required or permitted by state statute or federal law. | Assure public policy basis for dissemination of not public data; Protect individual privacy |
| 10 MS §138.163; MS §15.17, subd. 3 | Disposition of records | Dispose of and transfer records in accordance with statutory procedures | Ensure proper disposition of records preserved for legal or historical purposes |
| 11 MN Rules 1205.1500, subpart 1 | Plan for periodic review | Entity must formulate a plan for reviewing the administration of data practices | Ensure periodic determination of which data are necessary to maintain |
| 12 MN Rules 1205.1500, subparts 4, 5 | Modification of data handling procedures | Modify data collection and maintenance procedures to eliminate unnecessary data | Appropriate step following determination described above (11) |
| 14 MN Rules 1205.0500, subpart 3 | Parental access and notice to minors | Procedures for parents to access data about their minor children | Ensure parental rights while protecting minor's interests concerning parental access |

| MINNESOTA GOVERNMENT DATA PRACTICES ACT: COMPLIANCE CHECKLIST | | | |
|--|------------------------------------|---|---|
| Authority | Topic | Specific Obligation | Purpose |
| 15 MN Rules 1205.1300, subpart 4 | Authorized uses of data | Enumerate the authorized uses of data by category | Enable administrators to know how to respond to requests for data; Facilitate answers to questions about dissemination of data |
| 16 MN Rules 1205.1600 | Informed consent | Design forms for obtaining informed consent for new release or use of private data | Ensure that contents of informed consent forms comply with legal requirements |
| 17 MN Rules 1205.1000 | Responsible Authority | Each governmental entity must appoint a responsible authority by September 30, 1981 | Identify the entity's principal decision maker about data practices |
| 18 MS §13.05, subd. 13 | Data practices compliance official | Each governmental entity must appoint a compliance official by December 1, 2000 | Identify the person within the entity to whom questions or data practices problems may be directed |
| 19 MN Rules 1205.1200, subpart 2; MS §13.03, subd. 2 | Designees | Post the names of data practices designees, if appointed | Identify the other key data practices officials in each entity |
| 20 MN Rules 1205.1300, subpart 5 | Training | Responsible authority must train designees and other staff | Ensure compliance and avoid liability |

SECTION III
DUTIES OF THE RESPONSIBLE AUTHORITY:
ACCESS TO GOVERNMENT DATA BY
MEMBERS OF THE PUBLIC

The Minnesota Government Data Practices Act gives every member of the public the right to *see* and *have copies* of all public data kept by government entities. The MGDPA also places upon government entities various obligations relating to this right.

The rights and obligations described in this section do not apply to the right of a data subject to access data about herself or himself. These rights and obligations are described in Sections IV and VI.

What is the most basic requirement for properly responding to a data request?

In order to properly respond to requests for government data, each government entity must identify the types of data it maintains and to determine how each type of data is classified. (See How does one know how data are classified in Section II.)

Minnesota Statutes section 13.05, subdivision 1, specifically requires each entity to prepare a *public document* that identifies these data categories and classifications for data on individuals. Entities are not required to prepare a public document for data not on individuals.

The public document must contain the name, title, and address of the entity's responsible authority. Forms that are used by the entity to collect private and confidential data on individuals must be included in the document. The document must be updated annually. See Minnesota Rules, parts 1205.1200, and 1205.2000, subpart 5, an advisory form for the public document.

Are there other requirements relating to access to government data by the public?

Minnesota Statutes section 15.17, the Official Records Act, requires all government entities to make and maintain all records that are necessary to a full and accurate knowledge of their official activities. This requirement exists so that the public understands the actions taken by government, and the reasons for those actions. Section 13.03, subdivision 1, of the MGDPA requires government entities to keep records that contain government data in a way (or ways) that makes the data easily accessible for convenient use.

Who can make a data request?

Anyone may exercise the right to access public government data by making a data request.

To whom must a data request be made?

A data request must be made to the responsible authority or to the appropriate designee(s) specified in the entity's public document.

What kinds of data may a person request?

The person requesting government data may request access to specific types of data or data elements, to specific documents or portions of documents, to entire records, files or databases, or to *all* public data maintained by the entity.

Must a data request be made in writing?

Although the law does not specify the form in which a data request must be made, an entity *may* require that the data request be made in writing -- such as by letter, facsimile or e-mail transmission -- and may require the use of a form designed for this purpose. An entity requiring the use of a form must design the form so that it complies with the requirements of the MGDPA, and must establish how it will provide guidance to the public in using the form.

May an entity permit standing requests for data?

An entity may not prohibit or refuse a standing request for data. It may, however, limit the duration of a standing request or, after a period of time, confirm the requestor's desire to continue the standing request.

Must a government entity respond to a data request?

Once an entity has received a request, it must respond to the request.

What kind of response must the entity make and how soon must it respond?

The entity must respond to a data request appropriately and promptly. More than anything else, what is appropriate and prompt depends upon the scope of the request, and may vary depending upon such factors as the size and complexity of the entity, the type and/or quantity of data requested, the clarity of the data request, and the number of staff available to respond to the request.

How does an entity determine the appropriate response to a data request?

The first step in responding to a data request is to determine what specific data are requested. This may require the entity to seek clarification from the requestor. Although the entity may not require the requestor to provide identification, provide a reason for the request, or justify the request, the entity may request identifying information from the requestor if that information is necessary to fulfill the request.

The entity also must determine whether it maintains the requested data. The entity is not required by the MGDPA to provide data which it does not maintain. The entity also is not required to produce data in a particular form or format if the data are not maintained in that form or format. (The entity may provide data in a specific format pursuant to a data request for summary data. See, **What special requirements apply to requests for summary data?**, below.)

If the entity maintains the requested data, it then must determine how the data are classified. As described above, entities must know what data they maintain and how those data are classified in order to be able to determine whether the requested data may be made available to the requestor.

What is the appropriate response if the requested data *are not* public?

If the entity determines that the requested data are not public, it must inform the requestor. This may be done orally at the time of the request, or may be done in writing as soon as possible after the request is made.

When informing the requestor, the entity must cite the specific statutory section, temporary classification or specific provision of federal law that classifies the data. Making a general statement such as, “We can’t give you the data because of the data privacy act,” is not an appropriate response. The entity must cite the specific section of law (such as Minnesota Statutes section 13.43) which classifies the data as not public.

If the requestor asks for a written certification that the request has been denied, the entity must provide the certification, citing the specific statutory section, temporary classification or specific provision of federal law upon which the denial was based.

What is the appropriate response if the data *are* public?

If the entity determines that the data are public, it must provide the data to the requestor, regardless of who the requestor is or the reason for requesting the data.

What limits may an entity place upon access to the requested data?

The entity may limit access to data to reasonable times and places -- for example, during normal work hours, on certain days, at designated times for certain types of requests, at press conferences, or at negotiated times and/or locations.

What are the entity’s obligations if asked to explain the data provided?

The entity must explain the meaning of the data provided if the requestor asks for an explanation. This includes explaining the meaning of technical terminology, abbreviations, words or phrases.

The explanation must be provided in an understandable way. When providing explanations for non-English speakers or for persons with hearing or vision impairments, the entity may need to provide an appropriate interpreter.

May an entity refuse to provide copies of public data?

An entity may not refuse a request for copies of public data. If copies cannot be provided at the time of request, they must be supplied as soon as reasonably possible. If copies are requested in electronic form, and the entity maintains the data in electronic form, the data must be provided in electronic form.

May an entity assess a fee for *separating* public from not public data?

No.

May an entity assess a fee for *inspection* of public data?

No. *A fee may not be charged for inspection of government data.* This includes situations where:

- It is necessary for the entity to display computerized data on a terminal or print a copy of the requested data in order for the requestor to inspect the data,
- A person wishes to visually inspect a paper document or data kept in any other medium that may be inspected visually, or
- A person requests access to electronic data via her/his own computer equipment, and possibly prints copies or downloads data on her/his own equipment.

Just remember: Looking is free. (See, however, Minnesota Statutes section 169.09, subdivision 13(f), which permits law enforcement entities to charge a fee for access to traffic accident reports.)

May an entity assess a fee for providing *copies* of public data?

An entity may require a requestor to pay a fee for copies of public data or for electronically transmitting the data. The fee may include the actual costs of searching for and retrieving the data, including the cost of employee time, and for making, certifying and compiling, and electronically transmitting the data or copies of the data. The requirement that data be kept in a manner that makes them easily accessible for convenient use may limit the entity in charging for search and retrieval time.

Specific factors that may be considered in establishing a fee may be found at Minnesota Rules part 1205.0300, and in the document, FEES FOR PROVIDING COPIES OF PUBLIC DATA, included at the end of this section.

May an entity assess an additional fee for providing copies of data that have commercial value?

In certain circumstances, an entity may assess a fee in addition to the fee for providing copies of public data. The additional fee may be assessed when the entity receives a request for copies of data which have commercial value, and which are a substantial or discrete portion of or an entire formula, pattern, compilation, program, device, method, technique, process, data base, or system that was developed by the entity with a significant expenditure of public funds. The entity determines whether the data have commercial value.

The ability to assess an additional fee allows the entity to recover the cost of developing a system to maintain and manage electronic data. For example, the cost to Hennepin County to convert its property tax and land records from paper to electronic form constitutes the cost of development of its property information data base.

The additional fee must be calculated in a reasonable manner. To do so, the entity may consider the actual development costs incurred in producing the valuable data, and a reasonable estimate of how many requestors may be willing to pay the additional fee.

For discussion of specific factors that may be considered in establishing a fee, see Minnesota Rules, part 1205.0300 and the document, FEES FOR PROVIDING COPIES OF PUBLIC DATA, included at the end of this section.

What special requirements apply to requests for summary data?

Summary data are statistical records and reports that are prepared by removing all identifiers from private or confidential data on individuals. Summary data are public.

The responsible authority for an entity must prepare summary data upon the request of any person if the request is in writing and the requestor pays for the cost to prepare the data.

The responsible authority may delegate the preparation of summary data to anyone outside of the entity, including the requestor, if (1) that person/purpose is set forth in writing, (2) the person agrees not to release any of the private or confidential data used to prepare the summary data, and (3) the entity reasonably determines that the access will not compromise private or confidential data on individuals.

The entity may require the requestor to prepay the cost of preparing summary data.

FEES FOR PROVIDING COPIES OF PUBLIC DATA

Minnesota Statutes section 13.03 provides that, if a person requests copies or electronic transmittal of public government data, the responsible authority for the government entity may require the requesting person to pay the **actual costs** of **searching for** and **retrieving** government data, including the cost of **employee time**, and for **making, certifying, compiling** and **electronically transmitting** copies of the data, or the data themselves, *but may not charge for separating public data from not public data.*

Additional criteria for determining copy costs are set forth at Minnesota Rules, part 1205.0300, subpart 4. Various Commissioner's opinions, issued pursuant to Minnesota Statutes section 13.072, have established the following factors that may be used to determine how much an entity may charge for providing copies of public data.

THESE COSTS MAY BE INCLUDED, AS LONG AS THEY ARE *REASONABLE*:

- Staff time required to:
 - retrieve documents (The requirement that data be kept in a manner that makes them easily accessible for convenient use may limit the entity in charging for search and retrieval time)
 - sort and label documents, *if* necessary to identify the data to be copied
 - remove staples, paper clips
 - take documents to copier for copying
 - copy documents
- Materials (paper, copier ink, staples, diskettes, mag tapes, video or audio cassettes, etc.)
- Special costs associated with making copies from computerized data, such as writing or modifying a computer program to format data (keeping in mind that computerized data must be easily accessible for convenient use)
- Mailing costs
- Vehicle costs directly involved in transporting data to the appropriate facility when necessary to provide copies (for example, when the government entity is unable to provide copying services for photographs, oversize documents, videos, etc.)

THESE COSTS *MAY NOT* BE INCLUDED:

- Purchase of copier
- Maintenance of copier
- Normal operating expenses of computer
- Staff time required to:
 - Separate public from not public data
 - Open a data request that was mailed
 - Sort, label or review data, *if not* necessary to identify the data to be copied
 - Return documents to storage
 - Provide information about the data to the requester (ie, explain content and meaning of data)
- Administrative costs that are not related to copying
- Records storage
- Sales tax
- The entire cost of operating a multi-tasked computer for a measured unit of time, when fulfilling a request for copies was only one of the tasks performed during that unit of time.

SECTION IV

DUTIES OF THE RESPONSIBLE AUTHORITY: THE RIGHTS OF SUBJECTS OF GOVERNMENT DATA

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. The Legislature established these rights and controls because the decisions that government entities make, when using information about those individuals, can have a great effect on their lives.

These rights allow the data subject to decide whether to provide the data being requested; to see what information the entity maintains about that subject; to determine whether that information is accurate, complete and current and what impact the data may have (or have had) on decisions the entity has made; and to prevent inaccurate and/or incomplete data from creating problems for the individual.

This section is addressed to the responsible authority for the entity and explains the following rights of individual data subjects:

- The right to be given a notice (Tennessee warning) when either private or confidential data 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 Tennessee warning notice; or in ways to which the subject has 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.

The entity may use the information in Section VI to give to the data subject to inform data subjects of their rights and how to exercise them within that entity.

For a summary of the role of the government entity in protecting the rights of data subjects, see these documents at the end of this section:

- HOW A GOVERNMENT ENTITY MAY LAWFULLY COLLECT, STORE, USE AND RELEASE DATA ON INDIVIDUALS
- HOW THE MINNESOTA GOVERNMENT DATA PRACTICES ACT CONTROLS ACCESS TO PRIVATE DATA ON INDIVIDUALS
- HOW THE MINNESOTA GOVERNMENT DATA PRACTICES ACT CONTROLS ACCESS TO CONFIDENTIAL DATA ON INDIVIDUALS.

- THE TENNESSEN WARNING NOTICE
- MODEL INFORMED CONSENT FOR THE RELEASE OF GOVERNMENT DATA

Also see the document, *YOUR RIGHTS AS THE SUBJECT OF GOVERNMENT DATA*, at end of Section VI.

To actualize these rights, the MGDPA requires that the entity and the data subject each take certain actions. This section describes these actions by discussing four points at which they intersect:

- When the data are collected;
- When the data are used or released by the entity;
- When the individual exercises the right to access data about herself or himself; and
- When the data subject challenges accuracy and/or completeness of the data.

An important note about who may exercise the rights of the individual

Minnesota Rules, part 1205.0200, subpart 8, defines an individual as a living human being. Pursuant to section 13.02, subdivision 8, of the MGDPA, every individual is presumed competent to exercise all of the rights established by the MGDPA.

In the case of *individuals who are under the age of eighteen*, the MGDPA defines “individual” to include a parent or guardian, or someone who is acting as a parent or guardian in the absence of a parent or guardian. This means that a minor is presumed to be competent to exercise her/his rights under the MGDPA and so are her/his parent(s) or guardian(s).

An entity must presume that a parent may exercise the rights of the minor unless the responsible authority is provided with evidence that a court order specifically directs otherwise. Such court orders include those relating to divorce, separation or custody, and the termination of parental rights. Any other legally binding instrument may bar a parent from exercising the minor’s rights.

In some cases, a minor may have a legally appointed guardian who will be able to provide proof of appointment. In other instances, someone may be acting as a parent or guardian of the minor because the parent or guardian is absent. In that case, the entity must establish, based on knowledge of the particular situation, whether the person may exercise the rights of the minor.

Given various social and legal factors -- such as the existing variety of custody arrangements, blended families, etc. -- there may be more than one or two adults who are considered parents or guardians under the MGDPA.

In the case of *individuals who have been judged to be legally incompetent*, the MGDPA permits the individual’s legally appointed guardian to exercise that individual’s rights. A guardian wishing to exercise these rights must provide proof of legal guardianship in order to do so.

Actions at the point of data collection

What controls are placed on the collection and storage of data on individuals?

Government entities may **collect** and **store** *public, private* and/or *confidential* data on individuals *only* if necessary to administer or manage a program that is authorized by state law or local ordinance, or mandated by the federal government. An entity may not collect or store any data on individuals without proper legal authority, either express or implied.

What actions must an entity take before collecting and storing data on individuals?

Each entity must identify its specific legal authority(ies) for collecting and storing public, private or confidential data on individuals. It also must determine what types of data on individuals it collects or stores and how those data are classified.

The entity also must identify its specific legal authority(ies) for **using** and **disseminating** *private* and *confidential* data on individuals. These determinations are critical to complying with the Tennessee warning notice requirements, and providing data subjects with other rights, as discussed below. The determinations also provide information that must be included in the public document required by Minnesota Statutes section 13.05, subdivision 1.

What is a Tennessee warning notice?

Whenever an entity asks an individual to provide private or confidential data about her/himself, the entity must give that individual a notice -- sometimes called a Tennessee warning. See the document, THE TENNESSEN WARNING NOTICE, at the end of this section.

What must be included in the notice?

The Tennessee warning notice must inform the individual of:

- The purpose and intended use of the data. This is why the data are requested and how they will be used within the collecting entity;
- Whether the individual may refuse or is legally required to supply the data. The subject has the right to know whether or not s/he is required by law to provide the data requested;
- Any consequences to the individual of either supplying or refusing to supply the data. The entity is required to state the consequences known to the entity at the time when the notice is given; **and**
- The identity of other persons or entities that are authorized by law to receive the data. The notice must specifically identify recipients that are known to the entity at the time the notice is given.

When must the Tennessee warning notice be given?

The Tennessee warning notice is given at the point of data *collection*. The notice must be given whenever:

- A government *entity requests* data;
- The data are requested from an *individual*;
- The data requested are *private or confidential*; **and**
- The data are *about the individual* from whom they are requested.

All four of these conditions must be present before a Tennessee warning notice must be given.

When is a Tennessean warning notice *not* required?

The notice does not have to be given by law enforcement officers who are investigating a crime. The notice does not have to be given to the data subject when:

- the data subject is not an individual
- the subject offers information that has not been requested by the entity,
- the information requested from the subject is about someone else,
- the entity requests or receives information about the subject from someone else, or
- the information requested from the subject is public data about that subject.

How does an entity decide what to include in a Tennessean warning notice?

Preparation of a Tennessean warning notice begins by identifying the entity's legal authority(ies) for collecting, storing, using and releasing data on individuals. This should be done by, or in close consultation with, the entity's legal advisor. The specifics of these enabling authorities determine the reasons for collecting the data, how the data will be used, who is authorized to access the data, etc.

Each notice must be "tailored" to the requirements of the specific entity, program, or data collection event for which it is being prepared. Within any given entity, it is likely that more than one notice will be needed.

A model or sample Tennessean warning notice has not been included in this model policy because it is not possible to prepare one Tennessean warning notice that will cover all situations.

How does one know that a notice is complete?

In drafting the specific text of the notice, it can be helpful for the entity to pose each of the required elements in the notice as a question, and to answer each question very specifically, using the results from the research into legal authority(ies) for collecting and storing the data being requested. The answers can become the first draft of the notice.

Then ask and answer the same questions from the perspective of the individual data subject(s) to whom the notice will be given, and use the responses to revise and refine the draft as necessary.

When the text of the notice completely satisfies the questions of both the entity and the data subject, the notice most likely is complete and in compliance with legal requirements.

What are some practical suggestions for drafting a Tennessean warning notice?

In choosing words and phrasing for the Tennessean warning notice, it is hard to overemphasize the importance of using language that most people easily understand. The goal is to allow the data subject to make a meaningful decision to supply -- or not supply -- the information requested. Assuming the notice is complete and accurate, that choice can be meaningful only if the subject clearly understands what the entity communicates in the notice.

Communicating the contents of the notice may require preparation of the notice in more than one language, or it may require the provision of an interpreter. The entity should ensure that the subject has the opportunity to question anything in the notice and receive a clear explanation.

Does a Tennessee warning notice have to be given in writing?

The law does not require that the notice be given in writing. For practical and legal purposes, it is best to give the notice in writing (or in another recorded format). Although there is no law that requires an individual to sign an acknowledgment that s/he has received the notice, many entities ask the data subject to sign and date a written notice, in which case a copy of a written notice should be given to the data subject.

When information is collected over the phone, the notice should be provided orally. The entity should record such details as whether the notice was given, the date given, and the identity of the person giving the notice. If given orally, the subject also should be given the notice in writing, as described above, as soon as practicable.

What authority does the entity have when it has given the notice?

Once the proper notice has been given, the entity may lawfully collect, store, use and disseminate the data, as described in the notice.

What are the consequences of *not giving* the notice?

Data on individuals cannot legally be collected or stored if a proper Tennessee warning notice was not given. The Commissioner of Administration has issued numerous advisory opinions on this point. See, in particular, Opinions 95-028, 95-035, and 98-001.

Does this mean that the data *never* can be stored if a Tennessee warning notice was not given?

Not necessarily. Private or confidential data collected before August 1, 1975 (the effective date of the Tennessee warning notice requirement), may be stored for the reasons the data were collected. These data also may be stored for reasons of public health, safety or welfare, if the entity obtains the approval of the Commissioner of Administration.

Actions when data are used or released by the entity

What controls are placed on the use and dissemination of data on individuals?

Government entities may **use** and **disseminate** *private* or *confidential* data on individuals *only* if necessary to administer or manage a program that is authorized by state law or local ordinance, or mandated by the federal government. An entity may not use or disseminate any private or confidential data on individuals without proper legal authority, either express or implied.

This limitation on use and dissemination does not apply to public data on individuals because public data may be used or disseminated to anyone for any purpose.

What actions must an entity take before using or releasing private or confidential data on individuals?

Each entity must identify its specific legal authority(ies) for **using** and **disseminating** *private* and *confidential* data on individuals. The entity must use this information to comply with the Tennessean warning notice requirements discussed above.

What authority does the entity have after giving a proper Tennessean warning notice?

Once the notice is given, the entity may lawfully use and release private and confidential data on individuals, as described in the notice, without liability.

Can the entity use or release private or confidential data if it *has not given* a proper notice?

As a general rule, private and confidential data on individuals cannot legally be used or disseminated if a proper Tennessean warning notice was not given. The Commissioner of Administration has issued numerous advisory opinions on this point. See, in particular, Opinions 95-028, 95-035, and 98-001.

Does this mean that the data *never* can be stored, used or released if a Tennessean warning notice was not given?

Not necessarily. If an entity needs to use or release stored data in a way or for a purpose that was not included in the Tennessean warning notice, it may do so in one of these ways:

- **Informed Consent:** The entity may seek the data subject's informed consent to use or release the data in the new way. Obtaining the individual's informed consent is the primary way to recover from a situation where a complete or proper Tennessean warning notice has not been given. See the document, MODEL INFORMED CONSENT FOR THE RELEASE OF PRIVATE DATA ON INDIVIDUALS, included in this section.
- **Subsequent law:** If a federal, state or local law is passed after the notice has been given, and if that law requires or permits the use or release of the data in a way that was *not* included in the Tennessean warning notice, then the data may be used or released as permitted or required by the new law. The entity also must revise the notice to reflect the requirements of the new law.
- **Old Data:** Private or confidential data collected before August 1, 1975 (the effective date of the Tennessean warning notice requirement), may be used and released for the reasons the data were collected. These data also may be used or released for reasons of public health, safety or welfare, if the entity obtains the approval of the Commissioner of Administration.
- **Special Circumstances:** When it is not possible or practical to obtain the consent of the data subject(s), the entity may seek the approval of the Commissioner of the Department of Administration to use or release the data in a way or for a purpose that was not included in the Tennessean warning notice. For example, an entity might seek approval to use the data in a new way if consents would be required from hundreds or thousands of people, or if the data subject(s) is/are not able to give informed consent.

Actions relating to the subject's right to access data about herself or himself

Section 13.04 of the MGDPA gives specific rights to individuals who are the subjects of government data. One of these rights is the right of the data subject to access data about himself or herself.

The data subject has the right to ask and be told whether the entity maintains data about her/him, and whether those data are classified as public, private or confidential.

To exercise this right, the subject must make a request to the responsible authority for the entity or to a designee as specified in the public document required pursuant to 13.05, subd. 1. The entity may require that the request be in writing, including by letter, facsimile and e-mail transmission, and may require the use of a form designed for this purpose.

The entity may require the individual to provide identification in order to confirm that s/he is the subject of the data.

Criteria for deciding whether to require written data requests, or the use of a form, include the process established by the entity for handling data requests, the frequency of requests, the magnitude of a request or requests, and the sensitivity of data requested.

An entity requiring the use of a form must design the form so that it complies with the requirements described in this section, and must establish how it will provide guidance to the data subjects in using the form.

The entity must respond to such a request immediately, if possible, or within ten working days. Response includes informing the individual that s/he is the subject of data maintained by that entity and how those data are classified. It is important to note that, even though individuals cannot access confidential data about themselves, they do have the right to know whether confidential data are maintained by the entity.

The data subject has the right to see all public and private data about her/himself.

To exercise this right, the subject must make a request to the responsible authority, or the appropriate designee, as specified by the entity. The entity may require that the request be in writing, and may require the use of a form for this purpose as discussed above.

The entity may require the individual to provide identification in order to confirm that s/he is the subject of the data, and may require staff to be present at inspection in order to physically protect the data.

The entity must let the subject view the data immediately, if possible, or within ten working days of receiving the request, excluding Saturdays, Sundays and legal holidays. Inspection times and locations may be reasonably limited.

If the subject has requested data that are not accessible to him/her, the entity must inform the individual of this fact at the time of the request, and must cite the specific section of state or federal law that gives the entity the authority to withhold the data from the subject.

The data subject is entitled to see all public and private data which the entity maintains about him or her, but is not entitled to gain access to private or confidential data about other people which may appear in the records or files. The entity is required to determine what information relates to which person so that it may lawfully comply with requests for access to the data. The entity cannot refuse to give a data subject access to private or public data about her/himself just because not public data about other people are maintained in the record or file.

When an individual data subject requests data that include not public data about other individuals, the proper action for the entity is to remove from the requested data all private and confidential data about other individuals.

After the subject has reviewed data about her/himself, the entity is not required to show the data to the subject for six months unless:

- The entity collects or creates more data about the subject before six months have passed. If more data have been collected before the passage of six months, the subject has the right to inspect the data s/he originally viewed, as well as the newly-collected or created data; or
- The data subject has challenged the accuracy and/or completeness of the data, or is appealing the results of such a challenge, as described below.

Under certain circumstances, data about a minor data subject may be withheld from a parent or guardian.

A minor has the right the request that the entity withholds 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 and must be signed by the minor subject.

Upon receipt of the request, the responsible authority must determine whether honoring the request is in the best interests of the minor. In making this decision, the responsible authority must consider, at a minimum:

- Whether the minor is old and mature enough to explain the reasons for the request and to understand the consequences of making the request;
- Whether denying access to the data may protect the minor from physical or emotional harm;
- Whether there is a reason to believe that the minor's reasons for denying access to the parent(s) are reasonably accurate; and
- Whether the nature of the data is such that disclosing the data to the parents could lead to physical or emotional harm to the minor.

If the data concern medical, dental or other health services provided pursuant to Minnesota Statutes sections 144.341 to 144.347, and the data meet, at minimum, all of the above criteria, the data may be released to the parent only if failure to do so would seriously jeopardize the health of the minor subject.

A public educational entity or institution may not deny a parent access to education records or special education records about a minor child. See MODEL EDUCATIONAL DATA SHARING/ACCESS POLICY, published by the Minnesota Department of Administration, December, 1999.

The entity may not charge a fee for letting the subject see data about her/himself.

Looking is free. Even if the entity is required to produce a copy in order to permit the subject to view the data, it cannot assess a fee for doing so.

The subject has the right to be informed of the content and meaning of public and private data about her/himself upon request.

Upon the request of the data subject, the entity must explain the content and meaning of the data. This includes explaining the meaning of technical terminology, abbreviations, or words or phrases.

The explanation must be provided in a way the subject understands, including the use of another language, an interpreter, or other means. The entity must clearly inform the subject how to exercise this right.

The subject has the right to have copies of all public and private data about her/himself.

To exercise this right, the subject must make a request to the responsible authority, or to the appropriate designee, as specified by the entity.

The entity may require that the request be in writing, and may require the use of a form for this purpose as discussed above. Criteria for deciding whether to require written data requests, or the use of a form, include the process established by the entity for handling data requests, the frequency of requests, the magnitude of a request or requests, and the sensitivity of data requested.

The entity may require the individual to provide identification in order to confirm that s/he is the subject of the data.

The entity must provide the requested copies of the data immediately, if possible, or within ten working days of receiving the request.

If the subject has requested copies of data that are not accessible to him/her, the entity must inform the individual of this fact at the time of the request, and must cite the specific section of state or federal law that gives the entity the authority to withhold the data from the subject.

The data subject is entitled to have copies of all public and private data which the entity maintains about him or her, but is not entitled to access or copy private data about other people which may appear in the records or files. The entity is required to determine what information relates to which person so that it may lawfully comply with requests for copies of the data. The entity cannot refuse to give a data subject copies of private or public data about her/himself just because private data about other people are maintained in the record or file.

The entity may charge a fee for providing a data subject with copies of public and/or private data about her/himself.

The entity may charge only the actual and reasonable cost of making, certifying and compiling the copies. The entity may require payment of postage if mailing is requested.

Actions relating to the right of the data subject to challenge the accuracy and/or completeness of public and private data about her/himself.

The data subject has the right to challenge the accuracy and/or completeness of public and private data about her/himself.

If a data subject believes that public or private data about him/her are inaccurate and/or incomplete, s/he has the right to file a data challenge with the entity.

See the document, CHALLENGING THE ACCURACY AND/OR COMPLETENESS OF DATA THAT GOVERNMENT ENTITIES KEEP ABOUT YOU, at the end of this section.

The subject may challenge only *accuracy* and *completeness* of data. The Rules of the Department of Administration provide these definitions:

- *Accurate* means the data are reasonably correct and free from error.
- *Complete* means that the data describe all of the subject's transactions with the entity in a reasonable way.

Data may be inaccurate or incomplete because a wrong word, name, or phrase was used; because the data give a false impression about the subject; because certain information is not in the record; because certain information in the record should not be there; or for other reasons.

To challenge the accuracy and/or completeness of data, the data subject must communicate in written form to the responsible authority for the entity that the subject is challenging the accuracy and completeness of data the entity maintains about her/him. Written form includes communication via letter, e-mail message, or fax.

The written communication must identify the specific data being challenged; describe *why* or *how* the data are inaccurate or incomplete; and state what the subject wants the entity to do to make the data accurate or complete, i.e. add, alter or delete data.

Upon receipt of the challenge notice, the responsible authority, or someone within the entity designated by the responsible authority, must review the notice and the challenged data promptly. Although it is not required, appointing a disinterested person to review the challenge often enables a more expeditious resolution of the dispute.

Within 30 business days, the responsible authority must determine if the data are inaccurate or incomplete. The responsible authority may agree with all, part or none of the data challenge, and must notify the subject of the determination about the challenge.

If the responsible authority *agrees* that challenged data are inaccurate and/or incomplete, the entity must make the changes requested and try to notify anyone who has received the data in the past, including anyone named by the subject.

If the responsible authority *does not agree* that the challenged data are inaccurate and/or incomplete, the entity must notify the subject, who then has the right to appeal the entity's determination to the Commissioner of the Minnesota Department of Administration.

The data subject has the right to include a statement of disagreement with disputed data.

If an entity determines that challenged data are accurate and/or complete, and the data subject disagrees with that determination, the subject has the right to submit a written statement of disagreement to the responsible authority.

The form of the statement of disagreement is of the subject's choosing, and must be included with the disputed data whenever the disputed data are accessed or released.

If an entity determines that challenged data are accurate and/or complete, and the data subject disagrees with that determination, the subject has the right to appeal the entity's determination to the Commissioner of Administration.

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

If the entity has given the subject written notice of the right to appeal its determination, the subject must exercise the right to appeal within 60 calendar days. If the entity has not given the subject written notice of this right, the subject has 180 days within which to file an appeal.

The requirements for filing an appeal are set out at Minnesota Rules, part 1205.1600, and in the document, CHALLENGING THE ACCURACY AND/OR COMPLETENESS OF DATA THAT GOVERNMENT ENTITIES KEEP ABOUT YOU, at the end of this section.

How to Determine Whether a Government Entity May Lawfully Collect, Store, Use and Release Data on Individuals

Before collecting or storing any data on individuals, a government entity must ask:

Q: Is the collection or storage necessary for the administration and management of a program specifically authorized by the Legislature or local governing body, or mandated by the federal government? Has the relevant enabling authority been identified?

A: No -- *The data may not be collected or stored*

A: Yes- *Proceed to the next question.*

Q: Is the government entity asking an individual to supply private or confidential data about herself or himself?

A: No -- *The data may be collected without a Tennessee warning notice*

A: Yes - *A Tennessee warning notice must be given before the data are collected*

Before using or releasing any data on individuals, a government entity must ask:

Q: Are the data classified as private or confidential data on individuals?

A: No -- *The data are public and may be used or released*

A: Yes - *Proceed to the next question*

Q: Is the use or release necessary for the administration and management of a program specifically authorized by the Legislature or local governing body, or mandated by the federal government?

A: No -- *The data may not be used or released*

A: Yes- *Proceed to the next question*

Q: Was a Tennessee warning notice required when the data were collected?

A: No -- *Use or release the data*

A: Yes- *Proceed to the next question*

Q: Was the data subject informed (in a Tennessee warning notice) that the data would be used or released for this purpose?

A: Yes - *Use or release the data*

A: No -- *If the data are **confidential**, the data may not be used or released*

-- *If the data are **private**, the data subject's informed consent must be obtained before releasing or using the data. (See also Minnesota Statutes section 13.05, subdivision 4, for alternative authorities for use and release of private data.)*

HOW THE MINNESOTA GOVERNMENT DATA PRACTICES ACT CONTROLS ACCESS TO PRIVATE DATA ON INDIVIDUALS

This document explains, generally, when private data about an individual lawfully may be used or released and who has the right to access private data.

The Minnesota Government Data Practices Act (MGDPA), which is Chapter 13 of Minnesota Statutes, regulates access to government data. One way the MGDPA does this is by classifying data in ways that define who is legally authorized to see the information. For example, Minnesota Statutes section 13.43 classifies certain personnel data as private data on individuals.

Generally, private data may be accessed only by:

- the data subject
- staff of the entity whose work assignments reasonably require access (need to know)
- any person or entity authorized by law to access the data
- anyone who has the permission of the data subject
- anyone who has a court order to access the data

(See section 13.02, subdivision 12; section 13.05, subdivision 9; and Minnesota Rules, part 1205.0400.)

The MGDPA also controls access to private data by permitting disclosure of the data only if necessary to carry out a program or function specifically authorized by state or federal law. (Section 13.05, subdivision 3.) This authority may be explicitly established by law or it may be implied.

A third control is found in section 13.04, subdivision 2, which requires a government entity to give a notice whenever it asks an individual to supply private data about himself or herself. This notice is called a Tennessen warning and it must inform the individual of the following:

- Why the data are 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 of either supplying or refusing to supply the data; and
- Who else is authorized by law to receive the data.

Although the MGDPA does not require the Tennessen warning notice to be in writing, many entities include this notice on the forms used to collect information about individuals.

Last, section 13.05, subdivision 4, prohibits the use and release (dissemination) of private data for any purpose that was not stated in the Tennessen warning notice, unless

- the data subject has given permission (informed consent)
- a law allowing the new use or release is enacted after the data have been collected, or
- the new use or release is approved by the Commissioner of the Minnesota Department of Administration.

An informed consent must be in writing, must not be coerced, and must explain the reasons for the new use or release of the data and the consequences of that new use or release. (Minnesota Rules part 1205.1400.)

General summary:

If private data were *collected from the data subject*, the entity may use or release the data

- if the entity has the legal authority to do so **and** the use or release of the data was properly explained in the Tennessee warning notice
- or**
- if the data subject has consented to the new use or release.

If private data were *not collected from the data subject*, the entity may use or release the data

- if the entity has the legal authority to do so
 - or**
 - if the data subject has consented to the new use or release
- .

HOW THE MINNESOTA GOVERNMENT DATA PRACTICES ACT CONTROLS ACCESS TO CONFIDENTIAL DATA ON INDIVIDUALS

This document explains, generally, when confidential data about an individual lawfully may be used or released and who has the right to access confidential data.

The Minnesota Government Data Practices Act (MGDPA), which is Chapter 13 of Minnesota Statutes, regulates access to government data. One way the MGDPA does this is by classifying data in ways that define who is legally authorized to see the information. For example, Minnesota Statutes section 13.82, subdivision 5, classifies certain criminal investigative data as confidential data on individuals.

Generally, confidential data may be accessed only by:

- staff of the entity whose work assignments reasonably require access (need to know)
- any person or entity authorized by law to access the data
- anyone who has a court order to access the data

(See section 13.02, subdivision 3; section 13.05, subdivision 9; and Minnesota Rules, part 1205.0600.)

The MGDPA also controls access to confidential data by permitting disclosure only if necessary to carry out a program or function specifically authorized by state or federal law. (Section 13.05, subdivision 3.) This authority may be explicitly established by law or it may be implied.

A third control is found in section 13.04, subdivision 2, which requires a government entity to give a notice whenever it asks an individual to supply confidential data about himself or herself. This notice is called a Tennessen warning and it must inform the individual of the following:

- Why the data are 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 of either supplying or refusing to supply the data; and
- Who else is authorized by law to receive the data.

Although MGDPA does not require the Tennessen warning notice to be in writing, many entities include this notice on the forms used to collect information about individuals.

Last, section 13.05, subdivision 4, prohibits the use and release (dissemination) of confidential data for any purpose that was not stated in the Tennessen warning notice, unless

- a law allowing that use or release is enacted after the data have been collected, or
- the new use or release is approved by the Commissioner of the Minnesota Department of Administration.

General summary:

If confidential data were *collected from the data subject*, the entity may use or release the data

- if the entity has the legal authority to do so **and** the use or release of the data was properly explained in the Tennessean warning notice.

If confidential data were *not collected from the data subject*, the entity may use or release the data if the entity has the legal authority to do so.

THE TENNESSEN WARNING NOTICE
Minnesota Statutes Section 13.04, subdivision 2

| | |
|--|---|
| <p>The notice must be given when:</p> | <ol style="list-style-type: none"> 1. An individual 2. Is asked to supply 3. Private or confidential data 4. Concerning self <p>All four conditions must be present to trigger the notice requirement.</p> |
| <p>The notice does not need to be given when:</p> | <ul style="list-style-type: none"> • the data subject is not an individual • the subject offers information that has not been requested by the entity • the information requested from the subject is about someone else • the entity requests or receives information about the subject from someone else, or • the information requested from the subject is public data about that subject. |
| <p>Statements must be included that inform the individual:</p> | <ul style="list-style-type: none"> • Why the data are being collected from the individual 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 of either supplying or refusing to supply the data; and • The identity of other persons or entities authorized by law to receive the data. |
| <p>Consequences of giving the notice are:</p> | <p>Private or confidential data on individuals may be collected, stored, used and released as described in the notice without liability to the entity</p> |
| <p>Consequences of giving an incomplete notice, or <i>not</i> giving the notice at all, are:</p> | <p>Private or confidential data on individuals cannot be collected, stored, used or released for any purposes other than those stated in the notice unless:</p> <ul style="list-style-type: none"> • The individual subject of the data gives informed consent; • The Commissioner of Administration gives approval; or • A state or federal law subsequently authorizes or requires the new use or release. |

MODEL
INFORMED CONSENT FOR THE RELEASE OF GOVERNMENT DATA

For Government Entities Subject to the Minnesota Government Data Practices Act

History and Purpose of This Consent Form

This model consent form was prepared by the Information Policy Analysis Division of the Minnesota Department of Administration at the direction of the Legislature (1994 Laws of Minnesota, Chapter 647, Article 3, Section 8). The purpose of this consent form is to provide government entities in Minnesota with a vehicle for sharing information about individuals which complies with the requirements of state and federal laws that regulate access to government data.

When to Use This Consent Form

A consent form must be completed in order to disseminate private data on individuals when *a*) the release of the data is necessary to administer or manage a legally authorized program *and b*) one of the following conditions applies:

- The data subject was not given a Tennessee warning notice when the data were collected from that subject. (See below for an explanation of the Tennessee warning notice .)
- The release of the data is for a purpose or to a recipient which was not included in the Tennessee warning notice .
- A Tennessee warning notice was not given because the data were not collected from the data subject.
- In other situations where the consent of the data subject is required in order to release data about that subject.

These requirements are established by the Minnesota Government Data Practices Act (MGDPA), which is Chapter 13 of Minnesota Statutes. The MGDPA regulates the collection, creation, maintenance, use and dissemination of *all* data maintained by government entities in Minnesota and classifies data on individuals as public, private or confidential data. The MGDPA regulates access to private data on individuals as follows.

Minnesota Statutes section 13.02, subdivisions 8 and 12, define *private* data on individuals as data that are not available to the public but that are available to the subject of the data and to the parents of the data subject if the subject is a minor. Minnesota Rules, part 1205.0400, permits access by those within the collecting entity whose work assignments reasonably require access.

The MGDPA establishes several controls on the collection, use and dissemination of private data. Section 13.05, subdivision 3, limits the collection, use, storage and dissemination of private data on individuals to that necessary to administer and manage programs authorized by state or local government or mandated by the federal government.

Section 13.04, subdivision 2, requires that government entities give a notice to an individual whenever the entity asks the individual to provide private or confidential data about her/himself. The notice is called a Tennessee warning notice. The notice must state 1) the purpose and intended use of the data being collected, 2) whether the individual may refuse to supply the data or is required by law to supply the data, 3) the consequences of either supplying or refusing to supply the information, and 4) the identities of all those who are authorized by law to access the data.

Section 13.05, subdivision 4, limits the subsequent use and dissemination of private or confidential data, collected from an individual, to what was described in the Tennessee warning notice. If the entity wishes to use or release the data in a way *not* communicated in the Tennessee warning notice, this statutory section requires the entity to obtain the individual's *informed consent*. The standards for obtaining an informed consent are set out at Minnesota Statutes section 13.05, subdivision 4(d) and Minnesota Rules, part 1205.1400.

(In lieu of obtaining informed consent from the data subject, an entity may use or disseminate private data for a new purpose with the approval of the Commissioner of the Minnesota Department of Administration pursuant to Minnesota Statutes section 13.05, subd. 4(c) and Minnesota Rules, part 1205.1400.)

This model consent form meets all of the above standards and, as a general rule, may be used by any entity or person who is subject to the MGDPA. Entities may tailor this form to accommodate their specific needs; however, if alterations to the language on this form are significant, an informed consent obtained by using the altered form may fail to meet legal requirements. (For example, some members of family services collaboratives would like a consent form that requires completion only once and which accommodates all possible releases of data between or among a number of entities. Suggestions have included designing a check off system consisting of various boxes that represent entities and types of data. Although such a form might be convenient for entities that routinely share varying types of private data with other entities, it likely would not meet the legal standards for an informed consent.)

This consent form is not appropriate for use in situations where the specific form and content of an informed consent are dictated by law. (For example, see Minnesota Statutes section 13.05, subdivision 4(a) (1)-(7).)

CONSULT YOUR LEGAL ADVISOR BEFORE USING THIS OR ANY OTHER CONSENT FORM.

This is especially important where use of the consent form may present issues of compliance with other laws such as the Americans with Disabilities Act, or with the requirements relating to the release of data about minor children.

The model form, appearing on the next page, is addressed to the data subject. Instructions to government entities for completing the form appear on its reverse.

[IDENTITY OF AGENCY/ENTITY]

CONSENT FOR RELEASE OF INFORMATION

We are asking for your consent (permission) to release information about you to the entities or persons listed on this form. The information can't be released without your consent. This form tells you what information we want to release, or what information we want another entity to release to us. This form tells you the reasons we are asking for your consent. You have the right to look at all the information to be released and have copies of it. You should do this before you give your consent to release the information. If you want to look at the information or have copies of it, you must talk to (NAME AND HOW TO CONTACT).

You may consent to release *all* of the information, *some* of the information or *none* of the information. You may consent to release information to *all*, *some*, or *none* of the entities listed on this form.

If you give us your consent, we can release the information for (TIME PERIOD) or until (EVENT OR CONDITION). You may stop your consent any time before (THIS TIME PERIOD, EVENT, OR CONDITION). If you want to stop your consent, you must write to (NAME AND ADDRESS OF PERSON) and clearly say that you want to stop all or part of your consent. Stopping your consent will not affect information that already has been released because you gave your consent.

You do not have to consent to the release of any information that tells people that you or your child is disabled. If you are asking for help because of a disability, we may need information about the disability in order to help you.

If you have a question about anything on this form, please talk to (NAME) before you sign it .

-

[A.] I authorize the [entity] to release information about [name of data subject]. I understand that:

[B.] The information I agree to let you release is:

[C.] The information will be given to:

[D.] You are asking me to release this information so that:

[E.] If this information is released, what will happen is:

[F.] If this information is *not* released, what will happen is:

[G.] Signature of client _____ Date signed _____

[H.] Signature of parent or guardian _____ Date signed _____

[I.] Signature of person explaining this form _____ Date signed _____

and my rights _____ Date signed _____

INSTRUCTIONS TO ENTITIES FOR USING THIS FORM

These instructions correspond to the lettered sections on the reverse side of this form. Use plain language when tailoring this form to accommodate your entity's specific needs.

- A. Enter the complete name and address of the entity that maintains the information. Include any relevant program names, staff names, titles and phone numbers.
- B. Identify, *as specifically as possible*, the reports, record names or types of information or records that will be released.
- C. Identify the entity or entities to which the information will be released. Include the name and address of the entity. Include relevant staff names and titles. *Be specific.*
- D. Describe *specifically and completely* the purpose(s) for seeking the client's informed consent and the new use(s) to which the information will be put.
- E. Describe *specifically and completely* the consequences to the data subject of releasing the information. This means all of the consequences known to the entity at the time the consent is signed.
- F. Describe *specifically and completely* the consequences to the data subject of *not* releasing the information. This means all of the consequences known to the entity at the time the consent is signed.
- G. Instruct the client to sign the consent and enter the date on which the consent is signed.
- H. As a general rule, a parent or guardian's signature should be obtained when the client is under the age of 18 or has a legally appointed guardian; however, specific requirements for obtaining consent to release data in these circumstances vary. **Instructions for completing this portion of the form within your particular entity should be developed in consultation with your legal advisor.**

Consent Requirements Specific to Family Services Collaboratives

Outlined below are the conditions under which a consent is needed in order to share client data among members of a family services collaborative. These requirements are established by Minnesota Statutes section 124D.23.

- **Collaborative members that are subject to the MGDPA:**

- *County social services entities, schools or public health entities in the same collaborative:*

If you are a *county social services entity* or a *public health entity*, you do *not* need to secure the client's consent in order to inform each other whether you are serving an individual or family. As a general rule, however, you *must* obtain the client's informed consent in order to release *any other* client data to anyone else, including other members of the collaborative. (Check with your legal advisor or data practices advisor to determine whether a state or federal law requires or permits your entity to release the data. If this authority exists, you do not need to obtain the client's consent.)

If you are a *school district*, you may *not*, as a general rule, release *any* information about a student to anyone else, including other members of the collaborative, *unless 1)* the data have been designated as directory information in compliance with the policies and procedures that the federal Family Educational Rights and Privacy Act of 1974 (FERPA) requires school districts to follow, *or 2)* the parent (or the student, if the student is 18 years of age) has consented to the release. (Your district's policies and procedures, or legal advisor, should be consulted for specific guidance about releasing data about students or their families.)

- *Other members of the collaborative:*

You do *not* need to obtain the client's consent form to release client data to someone within your entity who has been identified by the entity as needing the data in order to do her/his job. As a general rule, however, you *must* obtain the client's informed consent in order to release *any* client data to anyone else, including other members of the collaborative. (Check with your legal advisor or data practices advisor to determine whether a state or federal law requires or permits your entity to release the data. If this authority exists, you do not need to obtain the client's consent.)

- **Collaborative members that are *not* subject to the MGDPA:**

You may collect and use client data as permitted by laws, codes of professional conduct, ethical standards, bylaws that are applicable to your entity, and in ways that are consistent with the promises made to clients. Consult your entity's policies and procedures, or legal advisor, before collecting or releasing client data.

Members of a Collaborative Organized Pursuant to a Joint Powers Agreement:

There are a number of questions relating to whether the status of collaboratives organized pursuant to a joint powers agreement differs from that of collaboratives that are not organized in this way. Your legal advisor should be consulted for specific advice.

Consent Requirements Specific to Children's Mental Health Collaboratives:

Minnesota Statutes section 245.493, subdivision 3, permits members of a children's mental health collaborative to share client data *only if 1) the client gives written informed consent and 2) the information sharing is necessary in order for the collaborative to carry out its statutory duties.* Proper use of this model consent form will fulfill the first requirement; however, members of children's mental health collaboratives *must* consult their legal advisors for a specific interpretation of the second requirement.

Challenging the Accuracy and/or Completeness of Data That Government Entities Keep About You

The Minnesota Government Data Practices Act gives you the right to challenge the accuracy and/or completeness of public and private data being maintained about you by any government entity in Minnesota. **There are two steps in this process.**

The **first step** is to make a data challenge to the government entity that maintains the data. If the entity agrees that the data are inaccurate or incomplete, the entity must change the data so they are accurate and/or complete.

If the entity does not agree with the data challenge, you have the right to take the **second step** and appeal the entity's determination to the Commissioner of the Minnesota Department of Administration.

It is important to follow the steps carefully and to do all of the things described below.

Step One: Making a Data Challenge

First, identify the government entity's responsible authority. This person, or a designee, must make sure that the entity complies with state data practices laws.

The responsible authority for a *state-level entity* (such as a state agency, board or commission) is the commissioner or chief executive officer for that entity. The responsible authority for a *county social services* entity is the director of that entity. For *cities, school districts, and other county offices*, the responsible authority is appointed by the governing board. Each *elected official* (such as a sheriff, a county auditor or the governor) is the responsible authority for his or her office.

Next, write to the responsible authority and ask to look at all public and private data the entity maintains about you. In order to protect your rights, it is very important that you make your data request to the responsible authority.

You may wish to make an appointment to inspect the data, which you may do free of charge. You also may ask for copies of the data. If you do, the government entity does have the right to charge you reasonable copying costs.

Review or inspect the data very carefully and make a note about any information that you believe is inaccurate or incomplete. *Inaccurate* means that the data are not correct or that there are errors in the data. For example, data might be inaccurate because a name is not spelled right, someone

is not quoted correctly, wrong facts are stated, or a name, time or date are wrong. *Incomplete* means that the data do not describe all of your contacts with the entity in a reasonable way. For example, data might be incomplete because words are left out of a report, a document is missing from a file, or an interviewer did not file a report about an interview.

Inaccurate or incomplete data can be a word, a sentence, a phrase, a paragraph, a number, a punctuation mark, etc. Sometimes it is difficult to decide exactly what makes the data inaccurate or incomplete.

The next step is to notify the entity's responsible authority that you are challenging the accuracy and completeness of data that the entity maintains about you. To protect your rights, be sure to say clearly that you are challenging data under the provisions of Minnesota Statutes section 13.04, Subdivision 4. This challenge notice must be done in writing -- such as by letter, e-mail or fax. If you are sending a letter, you may wish to send it by certified mail with return receipt requested. Be sure to keep a copy of your letters and any other correspondence.

In your challenge notice:

- Identify the data that you are challenging. There are many ways to do this. Because it is important to be very specific, a good way to identify the data is to make a copy of the document(s) containing the data, clearly mark the data you are challenging, and enclose the copy with your letter.
- Describe *why* or *how* the data are inaccurate or incomplete. Be very specific and write down as many reasons as you can.
- Say what you think should be done to make the data accurate or complete. For example, you may ask the entity to *add* a word, phrase, page, etc., to make the data complete or accurate. You may ask the entity to *change* the data to make them accurate or complete. You also may ask the entity to *remove* data from a file or *delete* some of the data to make the rest of the data complete and/or accurate. Again, be very specific and explain very carefully what you want the entity to do to make each piece of data accurate and/or complete.

When the responsible authority receives your challenge notice, s/he has 30 days to review it and to decide if the data are inaccurate or incomplete. The responsible authority may agree with all, part or none of your data challenge. The responsible authority must notify you of his or her decision.

If the responsible authority *agrees* with your challenge, the entity must make the changes you requested and try to notify anyone who has received the data in the past. This includes anyone you name.

If the responsible authority *does not agree* to correct or make changes to the data you have challenged, s/he must notify you. Then you have the right to take the second step in the process. The second step is to appeal the entity's decision (determination) about your challenge.

Step Two: Appealing the Entity's Decision About Your Challenge

If you do not agree with the results of your data challenge, you may appeal the entity's decision to the Commissioner of the Minnesota Department of Administration.

If the entity told you in writing that you have the right to appeal its decision about your data challenge, you must file your appeal within 60 days of the decision. If the entity did *not* tell you in writing that you have the right to appeal, you have 180 days from the date of the decision to file your appeal.

You must send your appeal to the Commissioner of Administration in writing (such as sending a letter, an e-mail message, a fax, etc.). You must include your name, address and a phone number (if any), the name of the entity that has the data you challenged, and the name of the responsible authority for that entity.

Describe the data that you believe are inaccurate or incomplete, and tell why you disagree with the entity's decision about your data challenge.

Also tell the Commissioner what you want to happen because of your appeal. For example: Do you want the entity to remove data from its files? Do you want the entity to change or add data?

Include a copy of your data challenge letter and copies of any other correspondence about your challenge that you have sent or received. Send your appeal to:

Commissioner of Administration
State of Minnesota
50 Sherburne Avenue
Saint Paul, MN 55155

If the Commissioner determines that your appeal meets all of the requirements in the law, the appeal will be accepted. At that point, the Department's Information Policy Analysis Division (IPAD) will try to resolve the dispute in an informal way, using conferences and/or conciliation. The IPAD also may suggest that you and the entity take the matter to mediation.

If the dispute can't be resolved informally, the Commissioner will, in most instances, order a hearing by an administrative law judge in the state Office of Administrative Hearings. The administrative law judge then hears the case and makes a recommendation to the Commissioner. The Commissioner reviews the recommendation and issues an order about whether the data are accurate and/or complete. You and the government entity each have the right to appeal the Commissioner's order to the Minnesota Court of Appeals.

You do not need to be represented by an attorney to appeal the results of a data challenge, but legal advice can be helpful because the administrative law process can be technical and complex.

*Information Policy Analysis Division, Department of Administration
305A Centennial Building, 658 Cedar Street
St. Paul, Minnesota 55155
Voice: 651.296.6733 or 1.800.657.3721 Fax: 651.205.4219
www.ipad.state.mn.us
July, 2000*

SECTION V YOUR RIGHTS AS A MEMBER OF THE PUBLIC TO ACCESS GOVERNMENT DATA

The Minnesota Government Data Practices Act gives you, and all other members of the public, the right to see and have copies of public data kept by or for the Commission. The Minnesota Department of Commerce is the official record keeper of the Commission and has all documents in docketed Commission proceedings. The law also controls how we keep government data and what we tell you when you ask to see the data that we have.

These rights and controls are:

The law says that all the data we have are public (can be seen by anybody) unless there is a state or federal law that classifies the data as *not public*.

We have a report that lists the kinds of data we keep about individuals, how each kind is classified, and what law classifies that kind of data. This report is called The Report of the Minnesota Public Utilities Commission on Private or Confidential Data on Individuals. If you want to see or have a copy of this report, contact Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147.

You have the right to look at all public data that we keep.

You may request and receive public information over the phone, in person, through the mail, or via e-mail. If it is not possible to give you the info in the way you ask, we will contact you to decide on another way to give you the information you asked for.

To look at public data that we keep, contact Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147. You can make your request during our normal working hours, which are 8:00 a.m. to 4:30 p.m.

You also have the right to make a standing request. Standing requests expire after one year.

You may ask to see:

- specific types of data or data elements;
- specific documents or portions of documents;
- entire records, files or data bases;
- all public data we keep.

In your request, you should say that you are making a data request under the MGDPA. Tell us as clearly as you can what information you want to see. If we are not sure exactly what information

you are requesting, we will ask you, but you don't have to tell us who you are or explain why you are asking for the data.

We will let you know as soon as we can whether or not we have the data you are asking for. If you are asking for public data and we have the data, we will let you see or have copies of the data right away. If we need more time to identify, find or copy the data you are asking for, we will let you know and we will tell you when we will be able to give you the data.

We don't have to give you data we don't keep.

If we don't have the data you are asking for, we will tell you right away. We do not have to collect or create data for you in order to respond to your request.

We may not have to give you public data in the form you want.

If we have the data you're asking for, but we don't keep the data in the form you want, we may not be able to give you the data in that form. If we can't put the data in the form you want, you may have the data in our format and convert it to the form you want. If we can put you the data in the form you want, we will let you know how long it will take us to provide the data and how much it will cost. Then you can decide if you want the data in that form or not.

We cannot charge you a fee for looking at public data.

You have the right to look at public data at no cost. We will let you look at computerized data on a computer screen, or print a copy, so that you can inspect the data at no charge.

You also may inspect public data on your own computer, and you may print or download the data using your own computer, at no cost.

We can't charge you a fee for separating public data from data that are not public.

You have the right to have public data explained in a way you understand.

If you have any questions about the meaning of public data that we keep, please contact [name, title, phone, and location of responsible authority or appropriate designee] and ask for an explanation. If you ask, we will provide an interpreter or find another way to explain the data.

You have the right to have copies of the public data that we keep.

You have the right to have a copy of any data that you have a right to see. This includes the right to have copies of all or parts of specific documents, files, records, data bases or types of data that we keep. If you ask for the copies in electronic form, and we keep the data in electronic form, we will give you the data in electronic form.

To ask for a copy of public data that we keep, contact Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147.

In your request, say that you are making a request for copies of data under the MGDPA. Tell us as clearly as you can what types of data or information you want copies of. If we have any question about the copies you are requesting, we will ask you. You don't have to tell us who you are or explain why you are asking for the data.

Once we have your request, we will provide the copies you asked for as soon as reasonably possible, depending on how many copies you are requesting and how many staff we have available to respond to your request.

We have the right to charge you a reasonable fee for providing copies.

We will, i.e., charge you a fee for making copies of the data you ask for. If you ask us to mail or fax the copies to you, the fee will, i.e., include postage or long distance phone charges. If you request a certified copy of a document, we will, i.e., charge you a fee to certify the document.

If you are requesting copies of data that have commercial value, we will charge you a fee in addition to the fee for the copies.

Our fee for providing copies is \$.25 per page. We require payment in advance.

You have the right to know why you can't see or get copies of data that are not public.

If the information you ask for is not public data, we will tell you that when you make your request, or we will notify you in writing as soon as possible. We also will tell you which specific law makes the information not public. If you ask, we will put this in writing for you.

You have the right to see and have copies of summary data.

Summary data are statistical records or reports that are prepared by removing all identifiers from private or confidential data on individuals. We will prepare summary data for you if you make a request in writing (letter, fax, e-mail, etc.) to Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147 and pay us what it costs to prepare the data.

We require prepayment. When we receive your request, we will contact you to make detailed arrangements to prepare the summary data.

We will let you or someone else prepare the summary data if:

- you explain in writing why you want to prepare the data;
- if you agree not to release any of the private or confidential data used to prepare the summary data; and
- if we determine that giving you access to private and confidential data will not compromise those data.

If you have any questions about how to access public data that we keep, please contact Burl Haar, Executive Secretary, who is our responsible authority, at 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147.

SECTION VI

YOUR RIGHTS AS THE SUBJECT OF GOVERNMENT DATA

The Minnesota Government Data Practices Act is a law that gives you important rights when we collect, create, keep, use or release data about you, and controls how we collect, use, and release data about you.

An important note about who may exercise your rights

The law defines an individual as a living human being and gives every individual all of the rights discussed in this document.

If you are a minor (which means that you are not yet eighteen years old), your parents or your guardian usually have the same rights as you do. This means that each of your parents or your guardian usually can look at and have copies of information we keep about you. Usually, they each have the right to give their consent to release the data about you. They each can challenge the accuracy and completeness of the data about you.

If you have no parents, or if your parents are not a part of your life, then the person who is caring for you has these rights.

In some cases, your parent or guardian does not have these rights. For example, we won't let your parent(s) or guardian exercise the rights the law gives you if there is a court order that takes these rights away from them. The court order might be about a divorce, separation, custody or some other matter, or it might take away the parental rights of your parent(s). Sometimes a state or federal law says that we can't let your parents see information about you.

If you have been appointed as the legal guardian for someone, you may exercise that individual's rights under the MGDPA. To do so, you must show proof of your appointment as legal guardian.

The law controls how we collect, keep, use and release data about you.

We can collect, keep, use and release private and confidential data about you only when a state or federal law allows or requires us to do it. The law also says we can collect, keep, use and release private and confidential data about you only if we need to in order to do our job.

The law says we have to give you a notice when we ask you to give us data about yourself.

When we ask you to give us private or confidential data about yourself, we will give you a notice. The notice sometimes is called a Tennessee warning notice. The notice tells you these things:

- We will tell you why we are collecting the data from you and how we plan to use the data.
- If there is a law that says you have to give us the data, we will tell you that. We also will tell you if you do not have to give us the data.
- We will tell you what might happen (consequences) to you if you give us the data.

- We also will tell you what might happen (consequences) to you if you do not give us the data.
- We will tell you what other people or entities have the legal right to know about, see or have copies of the data you give us. When we tell you this, we will be as specific as we can be.

Parts of the Minnesota Public Utilities Commission may collect information about you for different reasons and use it in different ways, so we may give you more than one notice, and the notices may be different. We will explain anything in the notice if you ask us.

Whenever we can, we will give you the notice in writing for you to read, and we will give you a copy of the written notice to keep. If we ask you for information over the phone, we will give you the notice when we talk to you, and we will give or send you a copy in writing as soon as we can after that. You do not have to sign the notice.

We only have to give you the Tennessee warning notice when we are asking you to give us private or confidential data about yourself. We *do not* have to give you the notice when:

- you give us information we haven't asked for,
- the information we are asking for is about someone else,
- the information we are asking for is public data about you, or
- the information is collected by a law enforcement officer who is investigating a crime. This includes police officers, and members of the fire department and sheriff's office.

The notice puts limits on what we can do with data we keep about you.

Usually, after we give you the Tennessee warning notice and you choose to give us the data we ask for, we will use and release the data only in the ways that were stated in the notice. There are some exceptions to this rule. These exceptions are:

- If a federal, state or local law is passed after we give you the notice and collect the data from you, and if that law says we may or must use or release the data in a way we didn't tell you about in that notice, then we will use or release the information in order to comply with the new law.
- Sometimes, after we collect private or confidential data about people for one purpose, we need to use or release that information for a different purpose. If there is no law that says we can use the data for the new purpose, we need permission from those people in order to use or release the information in the new way. Sometimes we can't get their permission. This might happen if we need to ask hundreds or thousands of people for permission to use data about them, or if the people can't give us their permission to use the data in the new way. If this happens, we may ask the Commissioner of the Minnesota Department of Administration to approve the new use or the new release of the information. We will use or release the data in the new way if the Commissioner approves.
- If we collected private or confidential data about you before August 1, 1975, we have the right to use, keep and release the data for the reasons we collected it. We also can ask the Commissioner of Administration for permission to use, keep or release the data to protect public health, safety or welfare.

- If a court orders us to release private or confidential data about you, we have to release the data.

If we need to use or release data about you in a new way, we need your permission.

If we need to use or release private data about you in a way that we didn't tell you about in the Tennessen warning notice, we will ask you for your informed consent. This has to be done in writing, so we will ask you to read and sign a consent form. A copy of the form we use is at the end of this document.

The consent form tells you:

- What information we want to release, or what information we want someone else to give us. You may consent to release *all* of the information, *some* of the information or *none* of the information that is listed on the form.
- The reasons we are asking for your consent and how the information will be used. You may consent to *all*, *some* or *none* of the uses/purposes listed on the form.
- Who will release the information and who will receive it. You may consent to release information to *all*, *some*, or *none* of the entities or people listed on the form.
- What will happen (the consequences) if you let us release or use the information in a new way.
- Who to talk to if you have any questions.

You don't have to let us use or release the information in the new way. Before you decide, you should look at the information. The consent form tells you who to talk to if you want to look at the information or have copies of it.

We have to explain everything on the consent form in a way that you understand. After you read and understand the consent form, we will ask you to sign it.

If you give us your consent, we can release the information for the length of time that is written on the consent form. You may stop your consent any time before that time is over. If you want to stop your consent, you must write to the person named on the form and clearly say that you want to stop all or part of your consent. Stopping your consent will not affect information that already has been released because you gave your consent.

We also will ask for your consent if someone asks us for private data about you and the law doesn't let us give the data to that person.

If *you* ask us to release private data about you to someone else, we will ask for your informed consent. If you give us your informed consent, we have to release the data in the way you ask.

We only ask for your informed consent to release *private* data about you. We don't need to ask for your consent to release public data about you because the law says we have to give public data to anyone who asks. The law does not give you the right to see confidential data about you or to let anyone else see the data.

You have the right to know if we keep data about you.

If you ask us, we will tell you if we keep information about you and we will tell you if the data are classified as public, private or confidential. To find out what information we keep about you, contact Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147.

You have the right to see data we keep about you.

If you ask us, we will show you the public and private data that we keep about you. Contact Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147.

In your request, tell us as clearly as you can what types of data or information you want to see. You have the right to see specific documents, files, records or types of data that we keep. You also have the right to ask for and see *all* of the public and private data about you that we keep.

Once we have your data request, we will show you the data right away if we can. If we can't show you the data right away, we will show you the data in no more than ten business days.

The law says we have to protect private data about you. For this reason, a member of our staff may be with you when you inspect the information.

After you have looked at the data you requested, we do not have to let you see the data again for six months, unless we collect or create more information about you before six months have passed. You do not have to wait for six months to see the data again if we have collected new data about you, or if you have challenged any of the data, or if you are appealing the results of that challenge. See the information below about how to challenge the accuracy and/or completeness of government data.

Note about access to data about minors:

If you are a minor, you have the right to ask us not to let your parents or guardian have private data about you. If you don't want us to give your parents information about you, you must write to Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147. Tell us why you don't want us to release the information to your parents; then sign your name, on your request. If you have any questions about how to do this, talk to Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147.

After you make your request, we have to decide if we will let your parents see the data. Before we make this decision, we have to think about:

- Is there a law that says we have to give the data to your parents?
- Do you have a good reason for asking us not to release the data?
-

- If we give your parents the data, would you be harmed in any way?
- Do you understand what will happen if we don't release the data?

We also have to think about whether it is in your best interest for us not to give the data to your parents.

We can't charge you a fee for looking at data about yourself.

You do not have to pay any money just to look at data about yourself, even if we have to make a copy of the information so that you can look at it.

You have the right to have public and private data about you explained to you.

If you have questions about the data we keep about you, please contact Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147. We will explain the data in a way you understand. If you ask, we will provide an interpreter or explain the data in some other way.

You have the right to have copies of data about yourself.

You have the right to have a copy of public and private data about yourself -- in other words, you may have a copy of any information you have the right to see. To get a copy of public or private data that we keep about you, contact Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147.

In your request, tell us as clearly as you can what data or information you want copied. You have the right to have copies of specific documents, files, records or types of data that we keep. You also have the right to have copies of *all* of the public and private data about you that we keep.

Once we have your request for copies, we will give you the copies right away if we can. If we can't give you the copies right away, we will give them to you in no more than ten business days.

We have the right to charge a fee for making the copies.

We will charge you a fee for making copies of the data you ask for. We can only charge you the actual cost of making and compiling the copies. If you ask us to mail or fax the copies to you, the fee will include postage or long distance phone charges. If you request a certified copy of a document, we will charge you a fee to certify the document.

You have the right to know why you can't see or get copies of data we keep about you.

If the information you want to see is not public or private data about you, we will tell you that, and we will tell you what part of the law says we can't show it to you.

You have the right to challenge the accuracy and/or completeness of data about you.

If you believe that public or private data that we keep about you are inaccurate and/or incomplete, you may file a data challenge with us. You may challenge only *accuracy* and *completeness* of data.

- *Accurate* means the data are reasonably correct and do not contain any errors.
- *Complete* means that the data describe the history of your contacts with us in a complete way.

For example, data may be inaccurate or incomplete if a wrong word, name, or phrase is used; if the data give a false impression about you; if certain information is missing from the record; or if certain information should not be in the record.

To make a data challenge, write a letter to Burl Haar, Executive Secretary, 651.201.2222, The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147 and say that you are challenging the accuracy and completeness of data we maintain about you.

Tell us very clearly what data you are challenging. Be very specific. For example, make it clear whether you are challenging a specific word, sentence, date, time, or name.

Tell us very clearly *why* or *how* the data inaccurate or incomplete. Be very specific and write down as many reasons as you can.

Tell us very clearly *what you think should be done* to make the data accurate or complete. For example, you may ask us to add information, change the data we have, or remove information from our records.

When we receive your letter, the law says we have 30 days to review it and the data you are challenging, to decide whether all, some or none of the data are inaccurate or incomplete, and respond to your challenge.

If we *agree* with all or part of your challenge, we will correct the inaccurate or incomplete data and try to notify anyone who has received the data in the past. This includes anyone you tell us has received the data.

If we *don't agree* with all or part of your challenge, we will tell you we believe that the data you are challenging are accurate and/or complete.

You have the right to include a statement with inaccurate and/or incomplete data.

If you believe that public or private data we have about you are not accurate or complete, you have the right to include a statement of disagreement with the data. If we release the disputed data to anyone else, we have to include your statement of disagreement with the data.

You can appeal our decision about your data challenge.

If you don't agree with our decision about your challenge, you may appeal the decision to the Commissioner of the state Department of Administration. When we respond to your challenge letter, we will tell you that you have the right to appeal our decision. You then have 60 days (about two months) to file your appeal. If we do not tell you about your right to appeal our decision, you have 180 days (about six months) to file your appeal.

Your appeal must be made to the Commissioner of Administration in writing (such as sending a letter, an e-mail message, or fax). Include your name, address, and a phone number, and make sure you name the Minnesota Public Utilities Commission and Burl Haar, Executive Secretary.

Say that you are appealing a decision we made about your data challenge (or your challenge to accuracy and/or completeness of data we keep about you). Tell the Commissioner what data you believe are inaccurate or incomplete. Also tell why you disagree with our decision.

Then tell the Commissioner what you want to happen because of your appeal. For example, do you want us to add, change or delete data in our files?

Include a copy of your challenge letter and any other letters about your challenge that you have sent or received. Send your appeal to:

Commissioner of Administration
State of Minnesota
50 Sherburne Avenue
Saint Paul, MN 55155

The Commissioner's staff will contact you about your appeal. The Commissioner's staff can be reached at

Information Policy Analysis Division (IPAD)
Minnesota Department of Administration
201 Administration Building, 50 Sherburne Avenue
St. Paul, MN 55155

Voice: 651.296.6733 or 1.800.657.3721

Fax: 651.205.4219

www.ipad.state.mn.us

If you have any questions about your rights, please contact Burl Haar, Executive Secretary, who is our responsible authority, at The Minnesota Public Utilities Commission, 121 7th Place East, Suite 350, St. Paul, MN 55101-2147; Tel. 651.201.2222.