SCOTT COUNTY

GUIDELINES AND PROCEDURES

FOR THE

MINNESOTA GOVERNMENT DATA PRACTICES ACT

Adopted by the Board of Commissioners of Scott County – October 26, 2010

MINNESOTA GOVERNMENT DATA PRACTICES ACT

Table of Contents

FORMS, INSTRUCTIONS and DATA PRACTICES NOTICE

MINNESOTA GOVERNMENT DATA PRACTICES ACT

Introduction

These guidelines and procedures provide direction in complying with those portions of the Minnesota Government Data Practices Act (MGDPA) that relate to *public access to government data* and to the *rights of subjects of data*.

The public access requirements are:

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

A BRIEF OVERVIEW OF THE MINNESOTA GOVERNMENT DATA PRACTICES ACT

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

Briefly, the Act regulates:

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

Government data is either *data on individuals or data not on individuals.* Data on individuals are classified as either public, private, or confidential. Data not on individuals are classified as public, nonpublic, or protected nonpublic. 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

COLLECTION OF GOVERNMENT DATA

What is the Minnesota Government Data Practices Act?

The Minnesota Government Data Practices Act (MGDPA), which is set forth in Chapter 13 of Minnesota Statutes (and Chapter 1205 of Minnesota Rules), is a state law that controls how government data are collected, created, stored, maintained, used, and disseminated.

What are government data?

Government data are all data, such as facts, information, reports, records, maintained in any recorded form by government entities, including counties. 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, CDs on charts, maps, etc. Government data normally do not include mental impressions, thoughts, or conversations since they are not recorded.

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.

A. Official records must be kept. Minn. Stat. § 15.17, subd. 1 requires all officers and agencies of the state, and all officers and agencies of counties, cities, and towns to make and keep all records necessary for a full and accurate knowledge of their official activities. As noted above, requirements for collecting, creating, maintaining, storing, and disseminating data are found in the Minnesota Government Data Practices Act and accompanying Rules. Links for locating the governing statute and rules can be found in Appendices B and C.

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

C. DEFINITIONS

1. **Annual Report.** The public document required by Minn. Stat. § 13.05, subd. 1, containing the name of the responsible authority and the individual designee, title and address, and a description of each category of record, file, or process relating to private or confidential data on individuals maintained by the government entity.

2. **Authorized Representative.** The individual, entity, or person authorized to act on behalf of another individual, entity or person. For the purposes of the

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

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

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

5. **Data Subject.** The individual or person about whom the data is created or collected.

6. **Designee.** Any person designated by a responsible authority (a) to be in charge of individual files or systems containing government data and (b) to receive and comply with requests for government data.

7. **Government Entity.** A state agency, a statewide system or a political subdivision.

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

9. **Informed Consent.** The written consent that must be given by a data subject to allow disclosure of private data regarding the individual.

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

11. **Political Subdivision.** Any county, statutory or home rule charter city, school district, and special district, a town exercising powers under Minn. Stat. Chap. 368 and located in a metropolitan area, and any board, commission, district or authority created pursuant to law, local ordinance, or charter provision. It includes any nonprofit corporation which is a community action agency organized to qualify for public funds, or any

nonprofit social service agency which performs services under contract to a government entity to the extent that the nonprofit social service agency or nonprofit corporation collects, stores, disseminates, and uses data on individuals because of a contractual relationship with a government entity.

12. **Representative of the Decedent.** The personal representative of an estate of a decedent during the period of administration, or if no personal representative has been appointed, or after discharge, the surviving spouse, any child of the decedent, or, if there are no surviving spouse or children, the parents of the decedent.

13. **Requestor.** The individual, entity, or person requesting access and/or copies of government data.

14. **Responsible Authority for Counties.** Each elected official of a county shall be the responsible authority of the respective office. An individual who is an employee of the county shall be appointed by the County Board to be the responsible authority for any data administered outside the departments of elected officials. For a statewide system, the responsible authority is the commissioner of any state department, or any executive officer designated by statute or executive order as responsible for such system.

15. **Rules.** "The Rules Governing the Enforcement of the Minnesota Government Data Practices Act." Minn. R., Chap. 1205. See Appendix B.

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

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

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

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

II. CLASSIFICATION OF GOVERNMENT DATA

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

A. DATA ON INDIVIDUALS

1. Public Data on Individuals

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

b. Data on Individuals is Public if:

1) A statute or federal law requires or allows the collection of the data and does not classify the data as private or confidential.

2) An application for Temporary Classification for private or confidential data on individuals is disapproved by the Commissioner of Administration.

3) The data are summary or statistical data derived from data on individuals.

4) Private or confidential data becomes public in order to comply with either judicial or administrative rules pertaining to the conduct of a legal action. (For example: Private or confidential data which is presented in or to the court and made public by the court.)

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

2. Private Data on Individuals

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

b. Tennessen Warning: Except for law enforcement investigations, a Tennessen Warning must be given when private data is collected from the subject of the data (Section IX.A describes the Tennessen Warning.)

A Tennessen Warning need not be given when private data are collected

from someone other than the subject of the data.

c. Data on Individuals is Private if:

1) A state statute or federal law expressly classifies the data as not accessible to the public, but accessible to the subject of the data.

2) A Temporary Classification of private has been approved by the Commissioner of Administration and has not expired.

3) If data are classified as both private and confidential by state or federal law, the data are private.

d. Access: Private data on individuals are accessible to:

1) The individual subject of the data or the representative as authorized in writing (if the subject is a minor, usually by the subject's parent or guardian).

2) Individuals, entities, or persons who have been given express written permission by the data subject. (Section IX.C. describes Informed Consent.)

3) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee.

4) Individuals, entities, or persons who used, stored, and released government data collected prior to August 1, 1975, with the condition that use, storage, and dissemination was not accessible to the public, but accessible to the data subject. Use, storage, and release of this data are limited to the purposes for which it was originally collected.

5) Individuals, entities, or persons for which a state, local, or federal law authorizes new use or new dissemination of the data.

6) Individuals, entities, or persons subsequent to the collection of the data and subsequent to the communication of the Tennessen Warning, when specifically approved by the Commissioner of Administration, as necessary to carry out a function assigned by law.

7) Pursuant to a court order.

8) Individuals, entities, or persons as otherwise provided by law.

3. Confidential Data on Individuals

a. Definition: Data on individuals are confidential if made not accessible by the public and not accessible to the individual subject of the data by state statute or federal law.

b. Tennessen Warning: Except for law enforcement investigations, a Tennessen Warning must be given when confidential data is collected from the subject of the data. A Tennessen Warning is not given when confidential data are collected from someone other than the subject of the data.

c. Data on Individuals are Confidential if:

1) A state or federal statute expressly provides that: (a) the data shall not be available to either the public or to the data subject, or (b) the data shall not be available to anyone except those agencies which need the data for agency purposes.

2) A Temporary Classification of confidential has been approved by the Commissioner of Administration and has not expired.

d. Access: Confidential data on individuals are accessible to:

1) Individuals, entities, or persons who are authorized by state, local, or federal law to gain access.

2) Personnel within the entity whose work assignment requires access as determined by the responsible authority, or the designee.

3) Individuals, entities, or persons who used, stored, and disseminated government data collected prior to August 1, 1975, with the condition that the data was not accessible to the individual subject of the data.

4) Individuals, entities, or persons for which a state or federal law authorizes a new use or new dissemination of the data.

5) Individuals, entities, or persons subsequent to the collection of the data and communication of the Tennessen Warning when specifically approved by the Commissioner of Administration, as necessary, to carry out a function assigned by law.

6) Pursuant to a court order.

7) Individuals, entities, or persons as otherwise provided for by law.

B. PUBLIC, NONPUBLIC, OR PROTECTED NONPUBLIC DATA NOT ON INDIVIDUALS

1. Public Data Not on Individuals

a. Definition: Public data not on individuals means data not on individuals which are accessible to the public.

b. Data Not on Individuals is Public if:

1) A statute or federal law does not expressly classify the data as not public.

2) An application for Temporary Classification for data as nonpublic or protected nonpublic is not approved by the Commissioner of Administration.

3) A statute requires the data to be made available to the public.

c. Access: Public data not on individuals are accessible to any person *regardless* of their interest in the data.

2. Nonpublic Data Not on Individuals

a. Definition: Nonpublic data not on individuals means data which are not public, but are accessible to the subject of the data, if any. As used here, the subject of the data means a person as defined in Section I.C., paragraph 10.

b. Data Not on Individuals is Nonpublic if:

1) A state statute or federal law classifies the data as not public, but accessible to the subject of the data, if any.

2) A Temporary Classification of data as nonpublic has been approved by the Commissioner of Administration.

c. Access: Nonpublic data not on individuals are accessible to:

1) The subject of the data, if any.

2) Personnel within the entity whose work assignment requires access as determined by the responsible authority or designee.

3) Individuals, entities, or persons authorized by statute or federal statute to gain access.

4) It is reasonable to conclude that access to the data should be limited

to entities or persons who have the legal authority for access, and to entity staff on a need-to-know basis, that a representative of the organization which is the subject of the data may access the nonpublic data and may consent to its release.

5) Pursuant to court order.

6) Individuals, entities, or persons as otherwise provided by law.

3. Protected Nonpublic Data Not on Individuals

a. Definition: Protected nonpublic data not on individuals means data which are not public and not accessible to the subject of the data, if any. As used here, the subject data means a person as defined in Section I.C., paragraph 10.

b. Data Not on Individuals is Protected Nonpublic if:

1) A state statute or federal law classifies the data as not accessible to the public and not accessible to the data subject.

2) The Temporary Classification of government data as protected nonpublic data has been approved by the Commissioner of Administration.

c. Access: Protected nonpublic data not on individuals are accessible to:

1) Personnel within the entity whose work assignment requires access as determined by the responsible authority or the designee.

2) Individuals, entities, or persons authorized by statute or federal law to gain access.

3) Pursuant to a court order.

4) Individuals, entities, or persons as otherwise provided by law.

C. SUMMARY DATA

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

2. **Data is Summary Data if:**

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

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

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

D. DATA ON DECEDENTS

1. Private Data on Decedents

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

b. Access:

1) Access is available to the personal representative of the estate during the administration or if no personal representative, the surviving spouse, any child of the decedent, or if no spouse or children, to the parent of the decedent.

2) A trustee appointed in a wrongful death action also has access to appropriate private data on decedents concerning the data subject.

2. Confidential Data on Decedents.

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

b. Access. Access to the data is the same as access to confidential data on individuals.

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

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

statute. Any person may bring an action in the district court located in the county where the data is being maintained or, in the case of data maintained by state agency, in any county, to authorize release of private data on decedents or confidential data on decedents. The court must examine the data and consider whether the harm to the surviving spouse, children, or next-of-kin of the decedent, the harm to any other individual identified in the data, or the harm to the public outweighs the benefit to the person bringing the action or the benefit of the public.

4. Private data on decedents and confidential data on decedents shall become public when ten (10) years have elapsed from the actual or presumed death of the individual and thirty (30) years have elapsed from the creation of the data. For purposes of this determination, an individual is presumed to be dead if either ninety (90) years elapsed since the creation of the data, or ninety (90) years have elapsed since the individual's birth, whichever is earlier, except that an individual is not presumed to be dead if readily available data indicates the individual is still living.

III. REQUEST FOR GOVERNMENT DATA

Refer to Section VI and the Information Disclosure Request form when copies are requested. While no fee shall be charged for viewing data, the actual costs of searching for and retrieving public data may be charged.

A. REQUEST FOR DATA - GENERAL - Upon request to the responsible authority or designee, an authorized person shall be permitted to inspect government data at reasonable times and places, and if the party requests, they shall be informed of the meaning of the data. *If the data requested are public data, no form or writing is necessary and the requestor is not required to identify themselves, state a reason for, or justify a request to gain access to public government data.* Sufficient information to identify or clarify may be asked for to facilitate access to the data. If requested, public data may be disclosed over the telephone.

If there is a request for copies of data and the county is not able to provide copies at the time of the request is made, copies shall be supplied as soon as reasonably possible.

Regardless of where the data originates, if it is in a government entity's possession, it is government data and subject to the access provisions of the law.

The Information Disclosure Request form shall be completed for all requests by the public for government data which is classified as other than public. See page 29.

B. REQUESTS FOR DATA ON INDIVIDUALS BY THE DATA SUBJECT

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

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

3. After an individual data subject has been shown the private data and informed of its meaning, the data need not be disclosed to that individual for six (6) months, unless a dispute or action is pending (concerning accuracy of data), or additional information has been obtained on that individual.

C. REQUESTS FOR SUMMARY DATA

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

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

3. The responsible authority or the designee shall:

a. Provide the summary data requested; **OR**

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

c. Provide access to the requestor to the private or confidential data so that the requestor can compile the summary data. Such access will be provided only when the requestor signs a non-disclosure agreement; **OR**

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

4. A non-disclosure agreement (see page 30) is used to protect the confidentiality of government data when the requestor of the summary data prepares the summary by accessing private or confidential data on individuals. A non-disclosure agreement shall contain at least the following:

a. A general description of the private or confidential data which is being

used to prepare summary data.

b. The purpose for which the summary data is being prepared.

c. A statement that the requestor understands that the requestor may be subject to the civil or criminal penalty provisions of the Act.

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

D. REQUESTS FOR GOVERNMENT DATA BY OTHER GOVERNMENT AGENCIES.

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

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

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

4. When practical and necessary, the requesting agency not listed on the Tennessen Warning (see page 32) shall obtain the informed consent from the data subject(s) for information classified as private or confidential.

E. HOW DATA PRACTICES APPLIES TO CONTRACTUAL LICENSING AND FUNDING RELATIONSHIPS WITH GOVERNMENT ENTITIES.

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

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

responsibilities.

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

4. 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 third party is subject to the MGDPA to the extent specified in the contract or the licensing agreement.

IV. INFORMATION DISCLOSURE REQUEST FORM.

A. INFORMATION DISCLOSURE REQUEST. The Information Disclosure Request provides a record of the requestor's identification information and the government data requested, as well as the action taken by the responsible authority, or the designee, and any financial transaction which occurs. See an example on page 29.

B. WHEN COMPLETED. The Information Disclosure Report should be completed for all requests by the public for government data *classified as private, confidential, nonpublic, and protected nonpublic and for all requests by other government agencies for which the not public data is not routinely shared or provided in the normal course of business.*

V. FEES FOR COPIES OF GOVERNMENT DATA.

Pursuant to the Minnesota Government Data Practices Act and Scott County Board resolution, and unless otherwise provided for by federal law, state statute or rule, fees for copies of government data shall be determined by departments based on the costs of providing such service, as set forth in the Scott County Fee Schedule set forth at http://www.co.scott.mn.us/CountyFeeSchedule. Fees shall be reasonable and consistent.

NOTE: FEES SHALL NOT BE CHARGED TO THOSE INDIVIDUALS WHO ONLY WISH TO VIEW OR INSPECT DATA.

NOTE: FEES MAY NOT BE CHARGED FOR SEPARATING PUBLIC FROM NONPUBLIC DATA.

A. COPIES PROVIDED AT NO CHARGE. When access is authorized, copies may be provided at no charge:

1. When another government agency or responsible authority requires or requests the record/document copies as part of the administration and

management of an authorized program and the copies are usually provided as part of the normal course of business.

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

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

B. COPIES PROVIDED WITH CHARGE. When access is authorized, copies shall be provided at the applicable Flat Rate or Special Rate in the following circumstances:

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

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

3. Public data on individuals and public data <u>not</u> on individuals, particularly when the requestor is not the subject of the data.

C. COPYING FEES. Copying fees shall be charged at the Flat Rate or the Special Rate for those records, documents, and publications covered in Section B above.

1. The Flat Rate shall be charged for all requested records, documents, and publications which are not otherwise identified in the Scott County Fee Schedule as described in Section V. The current Flat Rate to be charged is contained in Section E. The Flat Rate will be reviewed annually and updated, as necessary.

2. A Special Rate will be charged for copies of requested records, documents, and publications which are listed in the Scott County Fee Schedule by the department in which they are available.

3. A fee may be charged for remote access to data where either the data or the access is enhanced at the request of the person seeking the data, which may be determined on a case by case basis.

4. The actual costs may be charged of searching for and retrieving government data in response to a request for the data in electronic form, including the cost of employee time, for making, certifying and electronically transmitting copies of the data or the data, which may be determined on a case by case basis.

5. When copies are mailed, postage costs shall be added to the rates listed in Section E, unless alternative arrangements have been made.

D. COLLECTION OF COPYING FEES. Fees shall be collected before releasing copies unless prior arrangements have been made.

E. FEE SCHEDULE.

PHOTOCOPY FLAT RATE	25 cents per page if fewer than 100 pages
SPECIAL RATES	See Scott County Fee schedule at www.co.scott.mn.us/CountyFeeSchedule.
ELECTRONIC FORM OR REMOTE ACCESS	Individually determined

F. DISPOSITION OF FEES. Copying fees collected shall be deposited in the appropriate account with the county treasurer.

VI. ASSIGNMENT OF DESIGNEE.

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

VII. DUTIES OF THE RESPONSIBLE AUTHORITY OR DESIGNEE.

A. DATA PRACTICES ANNUAL REPORT.

1. The responsible authority shall prepare a public document on data categories. The public document will contain the responsible authority's name, title, address, and description of each category of record, file, or process relating to private or confidential data maintained by the County.

2. The public document shall be updated annually.

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

B. PROCEDURES FOR DISSEMINATION OF DATA.

1. The responsible authority shall ensure that each department establishes procedures to manage the dissemination of data. Collection, storage, use, and dissemination of private and confidential data shall be limited to what is

necessary for the administration and management of programs authorized or mandated by the state, county, or the federal government.

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

a. The data was collected prior to 1975, in which case the data may be used for the original purpose for which it was collected or for an additional purpose approved by the Commissioner of Administration.

b. There is specific authorization for the use in state, local, or federal law.

c. The additional use has been approved by the Commissioner of Administration as necessary to carry out a function designated by law.

d. The individual data subject has given an informed consent for the additional use of the data (see Informed Consent, Section IX., subd. C).

C. DATA PROTECTION.

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

VIII. ACCESS TO GOVERNMENT DATA

A. WHO CAN MAKE A DATA REQUEST?

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

B. TO WHOM MUST A DATA REQUEST BE MADE?

A data request must be made to the responsible authority or to the appropriate designee(s).

C. SUMMARY DATA

1. 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.*

2. The responsible authority may delegate the preparation of summary data to anyone outside of the entity, including the requestor, if:

a. That person's purpose is set forth in writing and the person agrees not to disclose or release any of the private or confidential data used to prepare the summary data; and

b. If the entity reasonably determines that the access will not compromise private or confidential data on individuals.

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

4. An example of a Non-Disclosure Agreement is included on page 30.

IX. RIGHTS OF DATA SUBJECT

A. TENNESSEN WARNING - Rights of Subjects of Data

1. Except for law enforcement investigations, every department that collects private and confidential data from an individual concerning that individual shall, prior to collecting the data, inform the individual of their rights as a subject of data. These rights are referred to as the "Tennessen Warning". The notice must be given whenever:

a. A government *entity requests* data;

b. The data is requested from an *individual*;

c. The data requested are *private or confidential*; **and**,

d. The data is *about the individual* from whom it is requested.

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

A Tennessen Warning is not required when private and confidential data is collected from an individual who is not the subject of the data.

2. The Tennessen Warning consists of the following information that must be communicated to the individual from whom private or confidential data concerning the individual is collected.

a. The purpose and intended use of the data. The reason why the data are requested and how it will be used within the collecting entity.

b. 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.

c. 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**

d. 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.

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

3. Tennessen Warnings may be either oral or written.

a. Oral communication. This is not the preferred method of communicating the Tennessen Warning. However, it may be necessary under some circumstances. If an oral communication is necessary, the specific language communicated must be in written form and contained in the departmental data practices procedures and the situation documented.

b. A written communication requiring the signature of the data subject (i.e., a signature attesting that the individual from whom private or confidential data is collected has read and understands their rights pertaining to the requested data). The Tennessen Warning may be included on the form that collects the private or confidential data.

4. A sample format for a Notice of Rights Tennessen Warning is on page 32.

B. NOTIFICATION TO MINORS

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

2. Upon receipt of the request, the responsible authority must determine whether honoring the request is in the best interests of the minor. The responsible authority must consider, at a minimum:

a. Whether the minor is old and mature enough to explain the reasons for the request and to understand the consequences of making the request;

b. Whether the requested denial of access to the data may protect the

minor from physical or emotional harm;

c. Whether there is a reason to believe that the minor's reason(s) for denying access to the parent(s) or guardian(s) is reasonably accurate; and

d. Whether the nature of the data is such that disclosing the data to the parents or guardians could lead to physical or emotional harm to the minor. Minn. Rule 1205.0500 contains the procedures for the release of data regarding minors.

C. INFORMED CONSENT

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

NOTE: Informed consent cannot authorize a new purpose or a new use of confidential data on individuals.

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

3. *All informed consents shall be in writing*.

4. Informed consent shall not be deemed to have been given by an individual subject of the data by the signing of any statement authorizing any person or agency to disclose information about the individual to an insurer or its authorized representative, unless the statement is:

a. In plain language;

b. Dated;

c. Specific in designating the particular persons or agencies the data subject is authorizing to disclose information regardinag the data subject;

d. Specific as to the nature of the information the subject is authorizing to be disclosed;

e. Specific as to the persons or agencies to whom the subject is authorizing information to be disclosed;

f. Specific as to the purpose or purposes for which the information may be used by any of the parties named in clause (e), both at the time of the disclosure and at any time in the future; and

g. Specific as to its expiration date, which should be within a reasonable period of time, not to exceed one (1) year, except in the case of authorizations given in connection with applications for life insurance or non-cancellable or guaranteed renewable health insurance and identified as such, two (2) years after the date of the policy.

5. The informed consent for the disclosure of alcohol and drug abuse patient records may be made only if the consent is in writing and expressly states the fact that the request is for alcohol or drug abuse patient records. It should contain the following:

a. The name of the program which is to make the disclosure;

b. The name or title of the person or organization to which disclosure is to be made;

c. The name of the patient;

d. The purpose or nature of information to be disclosed;

e. The extent or nature of information to be disclosed;

f. A statement that the consent is subject to revocation at any time, except to the extent that action has been taken in reliance thereon, and a specification of the data, event, or condition upon which it will expire without express revocation;

g. The date on which the consent is signed; and

h. The signature of the patient and, when required, of a person authorized to give consent.

6. A sample format and guide is included on pages 34-35.

D. PROCEDURES FOR COMPLYING WITH DATA REQUESTS FROM AN INDIVIDUAL DATA SUBJECT

The responsible authority shall ensure that each department establishes procedures to comply with requests for government data in an appropriate and prompt manner.

1. Upon request to the responsible authority, an individual shall be informed whether they are the subject of stored data on individuals, and whether it is classified as public, private, or confidential.

a. The responsible authority shall provide access to the private or public data upon request by the individual subject of the data.

b. An individual may contest the accuracy, current status, or completeness of public or private data. If the individual notifies the responsible authority in writing regarding the nature of the disagreement with the data, the responsible authority shall, within thirty (30) days, either correct the data and attempt to notify past recipients of inaccurate, incomplete, or out of date data, including recipients named by the individual, or notify the individual that the responsible authority believes the data to be correct. Subsequently, data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data.

2. The responsible authority shall prepare a public document, setting forth in writing the rights of an individual data subject and specific procedures in effect in the county for access by the individual data subject to public or private data on individuals.

a. The responsible authority shall comply immediately, if possible, with any request by an individual who is a data subject, or within (10) business days of the date of the request if an immediate response is not possible.

b. When a request is denied, the responsible authority must inform the individual data subject orally at the time of the request, and in writing, as soon thereafter as possible, and shall cite the state statute, temporary classification, or federal law on which the determination is based.

c. The responsible authority shall require the data subject to pay the actual costs of making and certifying copies of the data requested, except those exempted in Section V., subd. A, but may not be charged for viewing the data or separating private or confidential data from public data.

d. The responsible authority shall inform the individual data subject of the data's meaning, if requested to do so.

E. DENIAL OF REQUEST FOR DATA – COURT ORDERS AND SUBPOENAE

1. If the government agency determines that the requesting party is not entitled to data that is private or confidential (and informs the requesting party of that determination and the reason), the party seeking access to the data may bring a motion before the court to compel release. The agency may request an *in camera* (in chambers) review of the data by the court to make a determination what, if any data may be released, under what conditions and to whom.

2. Subpoena – a subpoena is not a court order. Service of a subpoena for requested data that the government agency determines is not releasable to the requesting party is not sufficient. In response to a subpoena, the court must be notified that the data will not be released without a court order. An example of a Notice is included at page 36.

F. IF THE COUNTY DETERMINES THAT DATA THAT ARE CHALLENGED ARE ACCURATE AND/OR COMPLETE, AND THE INDIVIDUAL SUBJECT OF THE DATA DISAGREES WITH THAT DETERMINATION, SHE OR HE HAS THE RIGHT TO APPEAL THE DETERMINATION TO THE MINNESOTA COMMISSIONER OF ADMINISTRATION.

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

2. The requirements for filing an appeal are set out at Minnesota Rules, Section 1205.1600.

3. The procedure when data are not accurate or complete.

a. An individual subject of the data may contest the accuracy or completeness of public or private data. To exercise this right, an individual shall notify, in writing, the responsible authority describing the nature of the disagreement. The responsible authority shall, within thirty (30) days, either:

1) Correct the data found to be inaccurate or incomplete and attempt to notify past recipients of inaccurate or incomplete data, including recipients named by the individual; or

2) Notify the individual that the authority believes the data to be correct. Data in dispute shall be disclosed only if the individual's statement of disagreement is included with the disclosed data.

4. The determination of the responsible authority may be appealed pursuant to the provisions of the Administrative Procedure Act, Minn. Stat. §§ 14.57 to 14.62 and Minn. R. 1205.1600, relating to contested cases. Upon receipt of an appeal by an individual, the Commissioner of Administration shall, before issuing the order and notice of a contested case hearing required by Minn. Rules, Chap. 14, try to resolve the dispute through education, conference, conciliation, or persuasion. If the parties consent, the Commissioner may refer the matter to mediation. Following these efforts, the Commissioner shall dismiss the appeal or issue an order and notice of hearing.

a. Data on individuals that have been successfully challenged by an individual must be completed, corrected, or destroyed by a state government entity without regard to the requirements of Minn. Stat. § 138.17.

b. After completing, correcting, or destroying successfully challenged data, a state agency, political subdivision, or statewide system may retain a copy of the Commissioner's order issued under Minn. R. Chap. 14 or, if no order was issued, a summary of the dispute between the parties that does not contain any particulars of the successfully challenged data.

X. ROLE OF THE COMMISSIONER OF ADMINISTRATION.

A. Pursuant to Minn. Stat. § 13.06, subd. 4, the Commissioner of the Minnesota Department of Administration is given the authority to approve new uses and disseminations of private and confidential data on individuals.

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

C. Section 13.072 of the MGDPA gives the Commissioner authority to issue opinions concerning the rights of data subjects and the classification of government data, which are advisory in nature. The Commissioner's Advisory Opinions may be found at www.ipad.state.mn.us.

XI. CONSEQUENCES OF NOT COMPLYING WITH THE MGDPA.

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

B. Minn. Stat. § 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.

XII. WHERE MORE INFORMATION CAN BE FOUND.

A. *Government entities always must look to their legal advisor(s) for guidance and legal advice on data practices issues.* 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.

1. Minnesota Statutes Chapter 13 (the MGDPA) may be found on the website of the Revisor of Statutes at: www.leg.state.mn.us/leg/statutes.asp.

2. Minnesota Rules, Chapter 1205, The Rules Governing Data Practices, promulgated by the Minnesota Department of Administration, may be found at the website: www.revisor.leg.state.mn.us/arule/1205.

SCOTT COUNTY

Non-Disclosure Agreement

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

2. Purpose for which summary data is being prepared:

3. I,_____,representing _____

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

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

_____ _____
Requestor of Data Date

_____ _____
Responsible Authority/Designee Date

THE NOTICE OF RIGHTS TENNESSEN WARNING
INSTRUCTION GUIDE

Minnesota Statutes § 13.04, subdivision 2

The notice must be given when:	1. An individual 2. Is asked to supply 3. Private or confidential data 4. Concerning self All four conditions must be present to trigger the notice requirement.
Statements must be included from the individual that inform the individual:	• Why the data is being collected and how the entity intends to use the data; • Whether the individual may refuse or is legally required to supply the data; • Any consequences to the individual of either supplying or refusing to supply the data; and • The identity of other persons or entities authorized by law to receive the data.
Consequences of giving the notice are:	Private or confidential data on individuals may be collected, stored, used, and released as described in the notice without liability to the entity.
Consequences on *not* giving the notice are:	Private or confidential data on individuals cannot be collected, stored, used, or released for any purposes other than those stated in the notice unless: • The individual subject of the data gives informed consent; • The Commissioner of Administration gives approval; or • A state or federal law subsequently authorizes or requires the new use or release.

YOUR RIGHTS

Your Right to Privacy

Minnesota's Government Data Practices Act, Minn. Stat. § 13.04(2) and (3) says you have the right to privacy. These laws also make it easier for you to see the information kept in your file.

Your Right to Know Why We Need Your Information

We need information on you for the following reasons:

1. To see if you may get a grant or medical help.
2. To decide how much your grant will be.
3. To see if you need help from Scott County Human Services.
4. To allow us to get Federal or State funds for the money, services or care that you receive.
5. To help us give you the correct employment or social services.
6. To help us give you the correct care and treatment of your medical or emotional problems.
7. To find out if you must pay a fee for the services you receive.
8. To meet Federal, State and County reporting rules.
9. To help schools get money for students.

Your Right to Know How We Use Your Information

The information we get will be used by our staff and other agencies allowed to use it by law. We will also use it to refer you to other benefit programs. If you move to another state or county, we will send some information to them. After we close your case, we will keep your file until the law lets us destroy it.

Your Right to Refuse to Give Information

You may refuse to give us the requested information. However, if you refuse to give it to us, you may not receive assistance or services.

Your Right to See Information

You may review all of the information we get about you except information classified as "confidential" by law. (Confidential information is information such as certain psychological or medical evaluations, records used to prosecute a crime, etc. We cannot share it the person who is the subject of the data.)

You have the right to disagree with information that you think is wrong. For more information about your data privacy rights, ask your worker.

Your Right to Know Who Else May See the Information

We may share the information we have about you with the following people or agencies:

1. People in this agency who need to see the information to do their jobs.
2. Anyone granted the right to see it by law. Anyone else who is included under a new law made after you sign this notice.
3. Other agencies under contract with Scott County Human Services.
4. The local Social Security Office.
5. Local, state and federal agencies that provide jobs and training.
6. The Minnesota Department of Health, if you or your family has a communicable disease.
7. Another county agency.
8. School districts.
9. The Child Support/Collections Department, Accounting Department and County Treasurer.
10. Your relatives who, by state law, are responsible for you.
11. Local housing agencies and food shelves.
12. A court who issues an order to give it information.
13. The courts for collection of an overdue fee.
14. Any city, county, state or federal civil or criminal investigators.

The above agencies will treat this information under the same privacy laws that we must use. No other person or agency may see this information without your written permission.

This notice applies to all future contacts you may have with us in person, over the telephone or by mail.

Your signature means that you know about your rights and that you understand them.

_____ _____

Your signature Date

_____ _____

Your signature Date

INFORMED CONSENT INSTRUCTION GUIDE

A. Enter the complete name and address of the entity that maintains the information. Include any relevant program names, staff names, titles and telephone 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 agencies 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 known consequences of releasing the information.

Describe specifically and completely the known consequences of *not* releasing the information.

G. Instruct the person 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 subject 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 the County Attorney's office.**

INFORMED CONSENT FOR THE RELEASE OF INFORMATION

I, _____

(Name of individual authorizing release)

authorize _____

(Name of individual, entity, or person holding record)

to disclose to _____

(Name of individual, entity, or person to receive the information)

the following information:

_____

for the purpose of:

_____

I understand that my records are protected under state and/or federal privacy laws and cannot be disclosed without my written consent unless otherwise provided for by state or federal law. I understand that once this data is released that it may be subject to further disclosure without my written consent. I also understand that I may revoke this consent at any time except to the extent that action has been taken in reliance on it and that in any event, this consent expires automatically in one year or as described below, whichever is earlier.

Specification of the date or condition upon which this consent expires:

_____

Executed this _____ day of _____ ,20 _____ .

_____

(Signature of individual authorizing release)

_____

(Signature of witness)

_____

(Signature of parent, guardian, or authorized representative, when required)

DATA PRACTICES NOTICE

I have been subpoenaed to testify before this Court. I have been advised by the Office of the Scott County Attorney to provide the following information to the Court:

> The data I have been requested to provide includes data which is classified as private data, as defined by Minnesota Statutes, Chapter 13, the Minnesota Government Data Practices Act. Pursuant to Minnesota Statute § 13.03 and Minnesota Rule 1205.0100, subp, 5, the Court's attention is called to this classification. The Data Practices Act requires that I may disclose this data only if the data subject has given written consent, a statute allows disclosure, or a court orders disclosure. If this Court orders me to provide this private data, I will do so.

APPENDIX A

MINNESOTA
GOVERNMENT DATA PRACTICES ACT

MINNESOTA STATUTES, CHAPTER 13

A copy of the current law.

Website: www.leg.state.mn.us/leg/statutes.asp

APPENDIX B

MINNESOTA
GOVERNMENT DATA PRACTICES ACT

MINNESOTA RULES, CHAPTER 1205

State of Minnesota
Department of Administration
Data Privacy Division

A current copy of this section.

Website: www.revisor.leg.state.mn.us./arule/1205

APPENDIX C

SCOTT COUNTY

Responsible Authorities and Designees

Responsible Authority: Gary L. Shelton
County Administrator

Designee: Lezlie Vermillion
Deputy County Administrator

Compliance Officer: Jeanne Andersen
Assistant County Attorney, County Attorney's Office

Responsible Authority for Divisions:

Sheriff's Office	Adam Pirri	Chief Deputy
Community Services	Lezlie Vermillion	Division Head
Employee Relations	Lori Huss	Division Head
Health & Human Services	Pam Selvig	Division Head
Information Technology	Jeff Peichel	Division Head
Ofc of Mgmt & Budget	Steve Jones	Division Head