CHIPPEWA COUNTY

GOVERNMENT DATA PRACTICES ACT

GUIDELINES AND PROCEDURES

TABLE OF CONTENTS

CHIPPEWA COUNTY

MINNESOTA GOVERNMENT DATA PRACTICES ACT

GUIDELINES AND PROCEDURES

INTRODUCTION

The Minnesota Government Data Practices Act regulates all government data collected, created, received, maintained, disseminated or stores by a state agency, political subdivision or statewide system regardless of it physical form, storage media or conditions of use.

Briefly, the Act describes: 1) What information can be collected, 2) With whom the information may be shared, 3) The classification of specific government data, 4) The duties of county personnel in administering the provisions of the Act, 5) Access and procedures for access to the information, 6) Procedures whereby information may classified as not public, 7) Civil penalties for violation of the Act, and 8) the charging of fees for copies of records.

The basis on which a determination of how government data is handled is the classification system. Government data is either data on individuals or data not on individuals. Data on individuals is classified as public, private, or confidential and data not on individuals is classified as public, nonpublic or protected nonpublic.

Since the Act and these guidelines and procedures are definition-dependent, a Glossary of Terms is contained in the back. (Exhibit I)

These guidelines and procedures are promulgated with intention of assisting department personnel in the determination of the correct classification and therefore handling of government data which are maintained by their departments. This manual is to be used in conjunction with the Minnesota Government Data Practices Act, MINN. STAT. 13.01, de seq. (as amended) and the Rules promulgated by the Commissioner of Administration, 2 MCAR, et al.

While these guidelines and procedures may be helpful to social service agencies, the Commissioner of the Minnesota Department of Public Welfare is the responsible authority for the government data collected, stored, used, and disseminated by the statewide public welfare system and, as such, may be procedures and forms which may vary from what is contained here.

RESOLUTION APPOINTING A COUNTY RESPONSIBLE AUTHORITY

State of Minnesota

County of Chippewa County

WHEREAS, Minnesota Statutes, Section 13.02, Subdivision 6, requires that Chippewa County appoint one person as the Responsible Authority to administer the requirements for collection, storage, use and dissemination of data on individuals within the county and,

WHEREAS, the Chippewa County Board of Commissioners shares the concern expressed by the legislature on the responsible use of all County data and wishes to satisfy this concern by immediately appointing an administratively and technically qualified Responsible Authority as required under the statue.

BE IT RESOLVED, the County Board of Commissioners appoints Jon Clauson as the Responsible Authority for the purpose of meeting all requirements of Minnesota Statutes, Sections 13.02-13.87, as amended, and with rules as lawfully promulgated by the Commissioner of Administration as published in the State Register on July 18, 1984.

ADOPTED BY CHIPPEWA COUNTY COMMISSIONERS ON JULY 18, 1984

ATTESTED TO: /s/ Marvin Teichert
Marvin Teichert

Chairman, County Board of Commissioners

CHIPPEWA COUNTY

RESPONSIBLE AUTHORITIES

The Minnesota Government Data Practices Act defines the responsible authority in a political subdivision as "…the individual designated by the governing body of that political subdivision as the individual responsible for the collection, use and dissemination of any set of data on individuals, government data or summary data, unless otherwise provided by State law" (M.S. 13.02 subd.16) The rules spell this out more clearly for counties.

> "Each elected official of the county shall be the responsible authority for his 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 offices of elected officials." (2 MCAR Section 1.202 subd. K-2)

CHIPPEWA COUNTY ELECTED OFFICIALS

Jon Clauson……Auditor/Treasurer
Jan Lenning……..Recorder
Stacy Tufto……..Sheriff
Dwayne Knutsen…….…….Attorney
Ron Jones……..……Coroner

Pursuant to M.S. 13.02 subd. 6 the Responsible Authority may assign one or more designees for each department. As the appointed responsible authority for Chippewa County. I name the below listed as "designees" for the purposes of administering the Minnesota Government Data Practices Act in Chippewa County.

Carol Schutz…….…… Assessor
? ……...……... License Bureau Director
Dennis Anderson……. Veterans Service Officer
Scott Williams…….……. Building Official
Steve Kubista……..…….…….. Highway Engineer
Leon Bechtle…….…..… Weed Inspector

The Commissioner of the Minnesota Department of Public Welfare is the responsible authority for any Welfare or Family Services data. Betty Christensen, Family Services Director serves as designee.

_____
Jon Clauson
Responsible Authority

I. COLLECTION OF GOVERNMENT DATA

The following regulates the collection of government data:

MINN. STAT. 13.03, subd. 1 Public data. All government data collected, created, received, maintained or disseminated by a state agency, political subdivision, or state wide system shall be public unless classified by statute, or temporary classification pursuant to section 13.06, or federal law, as nonpublic or protected nonpublic, or with respect to data on individuals, as private or confidential. The Responsible Authority in every state agency, political subdivision and statewide system shall keep records containing government data in such an arrangement and condition as to make them easily accessible for convenient use. Photographic, photostatic, microphotographic, or microfilmed records shall be considered as accessible for convenient use regardless of the size of such records.

II. CLASSIFICATION OF GOVERNMENT DATA

For the purpose of these guidelines, government data is divided into three types: 1) data individuals, which is classified as either public, private, or confidential, 2) data not on individuals, which is classified as either public, nonpublic or protected nonpublic, and 3) statistical or summary data derived from data on individuals. This classification, the criteria for classification and the description of who has access are as follows:

1. PUBLIC DATA ON INDIVIDUALS

A. DEFINITION: Public data on individuals means data on individuals, which is accessible to the public.

B. DATA ON INDIVIDUALS IS PUBLIC IF:

1. A statue or federal law substantially requires that certain data on individuals be made available to the public.

2. A statute or federal law requires the collection of data on individuals and does not classify the data as private or confidential.

3. The data is collected with any enable authority to do so and is not classified by either state statute or federal law even though the data is necessary for administration and management.

4. An application for “Temporary Classification” for private or confidential data on individuals is disapproved by the Commissioner of Administration.

5. The data is summary or statistical data derived from data on individuals.

6. Private or confidential data becomes public in order to comply with wither judicial or administrative rules pertaining to the conduct of legal actions (for

example, private or confidential data presented in court and made public by the court.)

C. ACCESS: Public data on individuals is accessible to the public regardless of their interest in the data. Public data is available to other government entities if needed for the administration and management of authorized programs.

2. PRIVATE DATA ON INDIVIDUALS

A. DEFINITION: Private data on individuals is data, which is not accessible to the public but accessible to the individual subject of the data.

B. 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 individual subject of the data.

C. ACCESS: Private data on individuals is accessible to:

1. Individuals, entities or persons who are given express written permission by the data subject.

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 are authorized by state, local or federal law to gain access.

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

5. Individuals, entities or persons for which a state, local or federal law authorizes a 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. A court, pursuant to a valid court order.

8. Individual, entities or persons as otherwise provided for by law.

D. TENNESSEN WARNING: A Tennessen Warning (Exhibit II) must be given when private data is collected from the subject of the data. This requirement shall not apply when an individual is asked to supply investigative date to a law enforcement officer.

A Tennessen Warning is not given when private data is collected from someone other that the subject of the data.

3. CONFIDENTIAL DATA ON INDIVIDUALS

A. DEFINITION: Data on individuals is confidential if statute or federal law makes it not accessible by the public and not accessible to the individual subject of the data.

B. DATA ON INDIVIDUALS IS CONFIDENTIAL IF:

1. A state statute or federal law 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.

C. ACCESS: Confidential data on individuals is accessible to:

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

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

3. Individuals, entities or persons who 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, local or federal law authorized 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. A court, pursuant to a valid court order.

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

D. TENNESSEN WARNING: A "Tennessen Warning" (Exhibit II) must be given when confidential data collected from the data subject. This requirement shall not apply when an individual is asked to supply investigative data to a law enforcement officer.

A "Tennessen Warning" is not given when confidential data is collected from someone other than the subject of the data.

4. SUMMARY DATA

A. DEFINITION: Summary Data means statistical records and reports derived from data on individuals but in which the individuals are not in any way identifiable.

B. DATA IS SUMMARY DATA IF:

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

2. Any list of number 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.

C. ACCESS: Unless classified by a "Temporary Classification", summary data is public and may be requested by and made available to any individual or persons. Summary data may be requested by a governmental entity if needed for the administration and management of authorized programs.

5. PUBLIC DATA NOT ON INDIVIDUALS

A. DEFINITION: Public data not on individuals means data not on individuals, which is 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 is "nonpublic" or "protected nonpublic" is disapproved by the Commission of Administration.

3. A statute or federal law substantially requires the data to be made available to the public.

4. The data is collected without any enabling authority to do so and is not classified by either statute or federal law.

C. ACCESS: Public data not on individuals is accessible to the public regardless of their interest in the data.

6. NONPUBLIC DATA NOT ON INDIVIDUALS

A. DEFINITION: Nonpublic data not on individuals means data, which is not public but is accessible to the subject of the data if any. As used here the "subject of the data" means an individual, partnership, corporation, etc.

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. The Commissioner of Administration has approved a "Temporary Classification" of data as non-public.

C. ACCESS: Nonpublic data not on individuals is accessible to:

1. The subject of the data, if any.

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

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

4. A court pursuant of a valid court order.

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

7. PROTECTED NONPUBLIC DATA NOT ON INDIVIDUALS

A. DEFINITION: Protected nonpublic data not on individuals means data, which is not public and not accessible to the subject of the data.

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 Commissioner of Administration has approved a "Temporary Classification" of government data as "protected nonpublic".

C. ACCESS: Protected nonpublic data not on individuals is accessible to:

1. Personnel within the entity who work assignment, as determined by the responsible authority or the designee, reasonably requires access.

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

3. A court, pursuant to a valid court order.

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

III. REQUESTS FOR GOVERNMENT DATA

1. REQUESTS FOR DATA-GENERAL: Upon request to the responsible authority or the designees, an authorized individual, entity or person shall be permitted to inspect and copy government data at reasonable times and places, and if the party request, he shall be informed of the data's meaning.

REGARDLESS OF WHERE THE DATA ORIGINATES, IF IT IS IN YOU POSSESSION IT IS GOVERNMENT DATA AND SUBJECT TO THE ACCESS PROVISIONS OF THE LAW.

The "Information Disclosure Request Form" shall be completed for any one of the following requests for government data. (Exhibit III)

A. For all requests by the public for government data classified as not public.

B. For all requests by other government agencies for which the data is not routinely shared or provided in the normal course of business.

C. For requests for all data (including public data) when a fee is assessed.

2. REQUESTS FOR DATA ON INDIVIDUALS BY THE DATA SUBJECT

A. Upon request and when access/copies are authorized, the designee shall provide copies the private or public data on individuals to the subject of the data or his/her authorized representative.

B. The designee shall comply immediately, if possible, or within five (5) working days of the date of request if immediate compliance is not possible. If the responsible authority or designee cannot comply with requests within that time, he/she shall inform the requestor, and may have an additional five (5) working days within which to comply with the request.

C. If access is authorized, the responsible authority or the designee must supply the requested data within ten working days.

3. REQUESTS FOR SUMMARY DATA

A. Unless classified by a "Temporary Classification" summary data derived from private or confidential data on individuals is public and the responsible authority or designee shall prepare the summary data upon the written request of an individual or person. The responsible authority shall prepare summary data upon the request of any government agency when required for the administration and management of authorized programs.

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

C. The responsible authority or the designee shall:

1. Provide the summary data requested as soon as reasonably possible; or

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

3. 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 form" (Exhibit IV; or

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

D. A non-disclosure agreement is used to protect the confidentiality of government data when the requestor of the summary data with prepare the summary by accessing private or confidential data on individuals. A non-disclosure agreement shall contain at lease the following:

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

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

3. A statement that the preparer (requestor) understands he may be subject to the civil or criminal penalty provisions of the Act in the event that the private or confidential data is disclosed.

4. A description of the civil and criminal penalty provision of the Act.

5. The signature of the requestor and the responsible authority designee or his representative.

4. REQUESTS FOR GOVERNMENT DATA BY OTHER GOVERNMENT AGENCIES

A. A responsible authority shall allow another responsible authority access to data classified as "not public" only when the access is authorized or required by state statute or federal law.

B. Access to data classified as public shall be limited to that necessary for the administration and management of authorized programs.

C. 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 required by state or federal law.

D. 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 if the data is classified as "not public".

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

5. REQUEST FOR ALL GOVERNMENT DATA

A. For requests from other than individual data subjects or government agencies or person, when access is authorized, the responsible authority or designee shall provide data on request.

B. If the responsible authority or designee is not able to provide copies at the time the request is made he shall supply copies as soon as reasonably possible.

IV. INFORMATION DISCLOSURE REQUEST FORM

1. INFORMATION DISCLOSURE REQUEST. The two-part "Information Disclosure Request" form as illustrated on (Exhibit III) provides a record of the requestor 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.

2. WHEN COMPLETED. The "Information Disclosure Request" should be completed for any one of the following:

A. For all requests by the public for government data classified as "not public".

B. For all requests by other government agencies for which the data is not routinely shared or provided in the normal course of business.

C. For requests for all data (including public data) when a fee is assessed.

3. GUIDELINES FOR USE

A. Instruct all records process employees on the correct of the form.

B. The "Information Disclosure Request" is divided into three sections.

1. Section A: Records requestor identification information.

For information that is classified as "not public", the responsible authority or designee shall insure that the requestor is, indeed, the subject of the data or his authorized representative. In order to insure this, the designee should require proof of identity including but not limited to a valid photo I.D. (such as a driver's license). In the case of the data subject's representative the date subject's signature approving release of "not public" information must be notarized.

2. Section B: Records the action taken by the designee. The responsible authority or designee always completes this section.

The "Authorized Signature" (item 12) should be signed by the responsible authority or the designee.

3. Section C: Records, when applicable, information pertaining to the charging and collection of fees for copying. Section V. of this manual describes fees for copies of government data and also provides the requestor with information that may be necessary to complete the transaction especially when all or part of the transaction is by mail

C. COPY DISTRIBUTION

1. The original copy should remain with the agency requested to provide access to data.

2. The pink copy of the completed form should be given to the requesting party. If there are any charges for copies, this will provide the requestor with a receipt.

V. FEES FOR COPIES OF GOVERNMENT DATA

Pursuant to the Minnesota Government Data Practices Act, unless otherwise provided for by federal law, state statute or rule, departments based on the costs of providing such

service shall determine fees for copies of government data. Fees shall be reasonable and consistent.

NOTE: FEES SHALL NOT BE CHARGES TO THOSE INDIVIDUALS WHO ONLY WISH TO VIEW THE DATA.

1. COPIES PROVIDED AT NO CHARGE. When access is authorized, copies may be provided at no charge under the following circumstances:

A. 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 business.

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

2. COPIES PROVIDED WITH CHARGE. When access is authorized, copies shall be provided at the applicable Flat Rate for all other requests including:

A. The media, including representatives of newspaper, radio, and television.

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

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

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

3. COPYING FEES. Copying fees shall be charged at the “Flat Rate” of $.25 per page unless a different fee is permitted by statute, (i.e. certified copies of court records).

4. COLLECTION OF COPYING FEES. Fees shall be collected before releasing copies. Under no circumstances will fees be "charged" and billed to the requestor.

A. When the estimated cost of providing copies of records, documents, and publications requested is $50.00 or more, the responsible authority or designee shall collect at least 50% of the estimated costs prior to making, certifying and compiling the copies.

B. When the estimated costs of providing copies of records, documents or publications is less that $50.00, the requested copies may be made prior to collecting the fees.

5. DISPOSITION OF FEES

A. Copying fees collected shall be turned over to the County Treasurer at least quarterly, or whenever collections exceed $50.00.

VI. DUTIES OF THE DESIGNEE

1. ASSIGNMENT OF DESIGNEES

The responsible authority, with the advice and cooperation of the department head, shall 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 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.

The responsible authority will provide designees with copies of the "Minnesota Government Data Practices Act", this Policies and Procedures Manual and other instructional materials as appropriate.

2. DATA INTEGRITY. The designee shall establish procedures to insure that all data on individuals maintained by the designee is accurate, complete and current for the purposes for which it is collected. For the purpose of this section:

A. "Accurate" means that the data in question is reasonably correct and free from error.

B. In accordance with rules and within 18 months of the effective date of the Rules, the responsible authority must provide for the preparation of a list or index to all data or types of data on individuals (i.e. public, private and confidential) collected, stored, used, or disseminated by the entity.

C. This list or index must include the identification of the statutes (s), federal law (s), or local ordinance (s) which authorize the programs or functions for which data or types of data are collected, or which authorize the actual collection, storage, or dissemination of the data or types of data on individuals. The list or index is a public document and will be updated annually by August 1st of each year.

D. The following descriptions and instructions for the various data elements may be helpful to you in completing the "Data Practices Annual Report" form.

1. Responsible Authority: Name, title and address. Enter the name, title and address of the responsible authority for the government data being reported.

2. Designee: Name, title and address. Enter the name, title and address of the designee who has been assigned in writing, to your unite.

3. Reporting Unit: Name and address. Enter the name of the department, division, and subdivision, or unit making the report.

4. Name of Record, File Process, for or Data Type: (Complete for public, private and confidential data.) Enter the name or title of the record, file, for the government data in terms that are readily understandable to the general public.

5. Enabling Authority: (Complete for public, private and confidential data.) The enabling authority is the state statute, federal regulation or rule that authorizes the actual data collections, storage, use, or dissemination.

6. Data Classification: (Complete for public, private and confidential data.) Enter Public, Private, or Confidential in the space provided. Remember, only a state statute, federal law to temporary classification can classify government data as not public.

7. Citation for Classification: (Complete for private and confidential data): Enter the citation for the Minnesota Statute, federal law or temporary classification which classifies the data as private or confidential.

8. Pre-August 1075 (Complete for public, private and confidential data.) Enter an "X" if the government data was collected prior to August of 1975. Private and confidential data collected prior to August 1, 1975 cannot be used, stored or disseminated for any purpose unless the enabling authority authorized that purpose, which was in effect at the time the data, was originally collected.

9. Post-August 1975 (Complete for public, private and confidential data.) Enter an "X" if the government data was collected after August 1, 1975. Private and confidential data collected after August 1, 1975 cannot be used for any purposes other that those stated to the individual at the time of collection except as provided by Minn. Stat. 13.03.

10. Current (Complete for public, private, or confidential data.) Enter an "X" if the government data is currently being collected.

11. Purpose and Use for Collection. (Complete for private and confidential data.) Enter a description of the purpose and use of the government data that is collected, used, disseminated, etc. by the reporting unit. In other words, why do you collect, use and store it?

12. Authorized Recipient (Complete for private and confidential data.) The authorized recipients are those individuals, entities or persons who are authorized by federal, state, or local law to gain access to the data. The authorized recipients are those individuals, entities or persons listed on your "Tennessen Warning".

E. When reporting public data on individuals it is not necessary to enter any information in the column "Citation for Classification" and "Authorized Recipients".

F. When reporting private and confidential data on the annual report include a sample of all form (s) used to collect that information, as required by Minn. Stat. 13.03.

G. The attached sample "Data Practices Annual Report" (Exhibit V) is reduced from 11" x 14". The sample form contains examples of how some types of data may be reported.

4. SECURITY SAFEGUARDS

A. The designee shall establish appropriate security safeguards for all records maintained by the designee containing data classified as "not public" to insure that access is gained by only authorized individuals, entities or persons.

B. The designee shall establish written procedures consistent with the Act to insure that private and confidential data is accessed by only authorized individuals.

5. WRITTEN PROCEDURES FOR REQUESTING DATA. The designee shall prepare and make available to the public upon request, a document setting forth in writing:

A. The rights of the data subject and the procedures for providing access to copies of public and private data concerning themselves.

B. The responsibilities of the designee in providing access to public and private on individuals.

C. Procedures whereby an individual may contest the accuracy and completeness of the public and private date concerning themselves.

D. Procedures whereby an individual may appeal the decision of the designee.

6. RECORD OF REQUEST. The designee shall:

A. Be prepared to receive and process requests to access and copy government data.

B. Keep accurate records of the number and type of requests received the response given and any resulting financial transactions.

C. "Information and Disclosure Request" forms have been developed to accomplish these ends.

7. CHARGING FEES. Unless otherwise provided for by federal law or state statute or rule, the designee shall charge reasonable fees for copies of government data based on the cost of providing such service. Fees for providing copies of government data shall be charged according to the guideline and procedures contained in Section V.

8. TENNESSEN WARNING – RIGHT OF SUBJECTS OF DATA

A. Every department that collects private and confidential data from an individual concerning him shall, prior to collection of the data, inform the individual of his/her rights as a subject of the data. These rights are referred to as the "Tennessen Warning". (Exhibit II) The example of the "Tennessen Warning in Exhibit II is one used for applications for employment, each department should draft their own warning describing what information may be collected and who the recipients of that information might be.

A "Tennessen Warning" consists of the following information that must be communicated to the individual from who private or confidential data concerning the individual is collected:

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

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

3. Any known consequences arising from the individual's supplying private or confidential data.

4. Any know consequences arising from the individual's refusing to supply private or confidential data.

5. The identity of other individuals, entities, or persons authorized by state or federal law to receive the data.

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

B. Depending upon the sensitivity of the information collected or the sensitivity of an individual to personal privacy, The "Tennessen Warning" may be:

1. An oral communication, while this is not the preferred method of communicating the "Tennessen Warning" it may be necessary under some

circumstances (i.e., collecting private or confidential data over the telephone). If an oral communication is necessary, the specific language communication must be in written form.

2. 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 his rights as a subject of the data.) The "Tennessen Warning" may be included on the form that collects the private or confidential data.

3. A written communication not requiring a signature. This may be for example, a brochure, booklet, pamphlet or a single sheet, which is handed to the individual prior to collecting the data. The "Tennessen Warning" may also be included on the form that collects the private and confidential data.

C. A sample of a Tennessen Warning" is contained in Exhibit II.

9. NOTIFICATION OF MINORS. Unless otherwise provided for by law (e.g., education and medical data), the designee shall provide minors from whom private or confidential data is collected with a notification that the minor individual has the right to request that parental access to the private data concerning the minor data subject is denied. The designee may require the minor data subject to submit a written request that the data be withheld. The written request from the minor shall set forth the reasons for denying parental access and shall be signed by the minor. Upon receipt of the written request the responsible authority or the designee shall determine if honoring the request to deny parental access is in the best interests of the minor.

10. INFORMED CONSENT

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

B. Private data may be used by and disseminated to any entity (e.g., political subdivision, government agency, etc.) if the individual subject or subjects have given their informed consent and the data is needed for the administration and management of programs authorized by state, local or federal law.

C. All informed consents shall be in writing.

D. 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 entity or person to disclose information about him or her to an insurer or its authorized representative, unless the statement is:

1. In plain language;

2. Dated;

3. Specific in designating the particular persons or agencies the data subject is authorizing to disclose information about themselves;

4. Specific as to the nature of the information he/she is authorizing is disclosed;

5. Specific as to the persons or entities to whom he/she is authorizing information to be disclosing;

6. Specific as to the purpose or purposes for which the information may be used by any of the parties named in clause 5, both at the time of disclosure and at any time in the future;

7. Specific as to its expiration date which should be within a reasonable period of time, not to exceed one year except in the case of authorizations given in connection with application for life insurance or noncancellable or guaranteed renewable health insurance and identified as such, two years after the date of policy.

E. The informed consent for the disclosure of alcohol and drug abuse patient records may be made only if the consent is in writing and contains the following:

1. The name of the program which is to make the disclosure.

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

3. The name of the patient.

4. The purpose or need for the disclosure.

5. The extent or nature of information to be disclosed.

6. 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 date, event, or condition up which it will expire without express revocation.

7. The data on which the consent is signed.

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

11. APPEALING THE DECISION OF THE DESIGNEE OR THE RESPONSIBLE AUTHORITY

A. A decision of the designee may be appealed to the appropriate responsible authority. A list of the responsible authorities for Chippewa County records is contained in Exhibit VI.

B. An individual who wished to appeal a decision of the designee must submit a written appeal to the responsible authority for the records in question. The designee shall make the name and address of the appropriate responsible authority available.

1. The name, addresses and telephone number of the appealing party.

2. The name of the designee or the individual who handled the initial request.

3. A description of the nature of the dispute includes a description of the information requested or in question.

4. A description of the desired result of appeal.

C. The decision of the designee or the responsible authority may also be appealed to the Commissioner of Administration. The procedures for this appeal are contained in the "Rules Governing the Enforcement and Administration of the Minnesota Government Data Practices Act."

D. Additionally, individual may, at any time bring action in district court. An action filed pursuant to this section may be commenced in the county in which the individual resides. If the court determines that an action is frivolous and without a basis in fact, it may award reasonable cost and attorney fees to the responsible authority.

EXHIBIT I

GLOSSARY OF TERMS

Minnesota Statue 13.02

Subdivision 1. Applicability. As used in this chapter, the terms defined in the section have the meaning given them.

Subdivision 2. Commissioner. "Commissioner" means the Commission of the Department of Administration.

Subdivision 3. Confidential data on individuals. "Confidential data on individuals" means data which is made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data.

Subdivision 4. Data not on individuals. "Data no on individuals" means all government data which is not data on individuals.

Subdivision 5. Data on individuals. "Data on individuals" means all government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data or any individual.

Subdivision 6. Designee. "Designee" means any persons designated by a responsible authority to be in charge of individual files or systems containing government data and to receive and comply with requests for government data.

Subdivision 7. Government Data. "Government data" means all data collected, created, received, maintained or disseminated by any state agency, political subdivision, or statewide system regardless of its physical form, storage media or conditions of use.

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

Subdivision 9. Nonpublic data. "Nonpublic data" means data not in individuals which is made by statute or federal law applicable to the data: a) not public; and b) accessible to the subject, if any, of the data.

Subdivision 10. Person. "Person" means any individual, partnership, corporation, association, business trust, or legal representative of an organization.

Subdivision 11. Political subdivision. "Political subdivision" means any county, statutory or home rule charter, city, school district, special district 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 pursuant to the Economic Opportunity Act of 1964, (P.L. 88-452) as amended, to qualify which performs services under contract to any political subdivision, statewide system or state agency, 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 state agencies, political subdivisions or statewide systems.

Subdivision 12. Private data on individuals. "Private data on individuals" means data which is made by statute or federal law applicable to the data: a) not public; b) accessible to the individual subject of that data.

Subdivision 13. Protected nonpublic data. "Protected nonpublic data" means data not on individuals which is made by statute or federal law applicable to the data: a) not public and b) not accessible to the subject of the data.

Subdivision 14. Public data not on individuals. "Public data not on individuals" means data which is accessible to the public in accordance with the provisions of section 13.03.

Subdivision 15. Public data on individuals. "Public data on individuals" means data which is accessible to the public in accordance with provisions of section 13.03.

Subdivision 16. Responsible authority. "Responsible authority" in a state agency or statewide system means the state official designated by law or by the commissioner as the individual responsible for the collection, use and dissemination of any set of data on individuals, government data, or summary data. "Responsible authority" in any political subdivision means the individual designated by the governing body of that political subdivision as the individual responsible for the collection, use, and dissemination of any set of data on individuals, government data, or summary data, unless otherwise provided by state law.

Subdivision 17. State agency. "State Agency" means the state, the University of Minnesota, and ny office, officer, department, division, bureau, commission, authority, district or agency of the state.

Subdivision 18. Statewide system. "Statewide system" includes any record-keeping 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 that one of its political subdivision or any combination of state agencies and political subdivision.

Subdivision 19. Summary data. "Summary data" means statistical records and reports derived from data on individuals but in which individuals are not identified and from which neither their identities or any other characteristic that could uniquely identify an individual is determinable.

EXHIBIT II

CHIPPEWAM COUNTY

SAMPLE TENNESSEN WARNING

In accordance with the Minnesota Government Data Practices Act, Chippewa County is required to inform you of your rights as they pertain to the private information collected from you. Private data is that information which is available to you, but not to the public. The personal information we collect about you is private.

Minnesota Statutes 13.01 to 13.87 on Government Data Practices require that you be informed that the following information which you are asked to provide on the application for employment is considered private data: 1) Name, 2) Home address, 3) Home phone number, 4) Social Security number, 5) Date of birth, 6) Conviction record, 7) Sex, 8) Age group, 9) Disability type.

We ask this information for the following reasons: 1) to distinguish you from all other applicants and identify you in our personnel files; 2) to enable us to verify that you are the individual who makes the application; 3) to enable us to contact you when additional information is required, send you notices and/or schedule you for interviews; 4) to determine if you meet the minimum age requirements (if any); 5) to conduct proper investigations if you are applying for a position; 6) to determine whether or not your conviction record may be a job related consideration affecting your suitability for the position you applied for; 7) to enable us to ensure your rights to equal opportunities; 8) to meet federal and state reporting requirements.

The data supplied by you may be used for such other purposes as may be determined to be necessary in the administration of personnel in Chippewa County and the policies, rules, and regulations promulgated pursuant thereto.

FURNISHING SOCIAL SECURITY NUMBERS, DATE OF BIRTH (unless a minimum age is required), SEX, AGE GROUP, AND DISABILITY DATA IS VOLUNTARY, BUT REFUSAL TO SUPPLY OTHER REQUESTED INFORMATION WILL MEAN THAT YOUR APPLICATION FOR EMPLOYMENT MAY NOT BE CONSIDERED.

Private data is available only to you and to other persons in the County Offices who have a bonafide need for the data. Public data is available to anyone requesting it and consists of all data furnished in the employment process which is not designated in this notice as private data.

Witness my signature that I fully understand the contents of this warning.

Date_____ _____

Signature of Applicant

EXHIBIT III
CHIPPEWA COUNTY
INFORMATION DISCLOSURE REQUEST &
CONSENT FOR THE RELEASE OF INFORMATION

A. REQUESTOR COMPLETE: DATE OF REQUEST _____

1. REQUESTORS NAME_____
2. ADDRESS _____
_____
3. DESCRIPTION OF THE INFORMATION REQUESTED
_____
_____
_____

4. REQUESTOR SIGNATURE_____

5. I, _____ hereby authorize Chippewa County to
to release the above described information to _____
_____ Data subjects signature_____
Subscribed and sworn to before me this _____ day of _____ 20____

B. DEPARTMENT/DIVISION COMPLETE:

6. DEPARTMENT/DIVISION NAME_____
7. REQUEST HANDLED BY _____
8. REQUEST TYPE _____IN PERSON _____ MAIL _____ PHONE
9. REQUESTED BY _____ SUBJECT OF DATE _____NOT SUBJECT OF DATA
10. THE INFORMATION REQUESTED IS CLASSIFIED_____PUBLIC____PRIVATE CONFIDENTIAL
_____NON-PUBLIC_____PROTECTED NON-PUBLIC
11. REQUEST_____APPROVED_____DENIED_____APPROVED IN PART
12. AUTHORIZED SIGNATURE_____
13. REMARKS/COMMENTS (if requested data is classified so as to deny access to the requestor cite authority or reason. Also enter any other remarks/comments appropriate.) _____
_____
_____
_____

C. DEPARTMENT/DIVISISON COMPLETE WHEN FEES ARE ASSESSED
(A receipted copy of this form is to be provided to the requestor each time money is received.)

14. Fees: Flat rate_____x .25 = TOTAL DUE _____

CHIPPEWA COUNTY RESERVES THE RIGHT TO RERQUIRE A 50% PREPAYMENT OF THE ESTIMATED TOTAL COPYING COSTS IF OVER $50.

I have received from the above named, the amount indicated opposite my signature in payment for providing the data.

TOTAL AMOUNT DUE $ _____RECEIVED BY_____DATE_____
__
PREPAID AMOUNT $_____RECEIVED BY _____DATE_____
BALANCE DUE $_____ RECEIVED BY _____ DATE_____
__

MAKE CHECK OR MONEY ORDER PAYABLE TO JON CLAUSON, CHIPPEWA COUNTY TREASURER

IF MAILED RETURN ENTIRE FORM AND ANY FEES TO:
_____
_____
_____

EXHIBIT IV
CHIPPEWA COUNTY
NON-DISCLOSURE
AGREEMENT

I, _____, hereby acknowledge receipt of the following private or confidential data:

_____

_____

_____

_____

This information will be used to prepare the following summary data:

_____

_____

_____

_____

I, _____ understand that I may be subject to the civil or criminal penalty provision of the Data Practices Act in the event that the private or confidential data is disclosed sufficiently to uniquely identify individual data subjects.

> MINN. STAT. 13.08 entitled Civil Remedies provides in part that any political subdivision, responsible authority or state agency which violates any provision of this chapter is liable to the person who suffers any damage as a result of the violation. The person damaged may also bring an action to cover any damages sustained, plus costs and reasonable attorneys fees. In the case of a willful violation, exemplary damages of not less that $100.00, nor more that $10,000.00 for each violation may be assessed.
>
> MINN. STAT. 13.09 entitled penalties provides in part that any person who willfully violates the provisions of 13.02 to 13.04 or any rules or regulations promulgated thereunder is guilty of a misdemeanor which is punishable by a maximum fine of $700.00 and/or 90 days in jail.

Dated _____ _____
Signature of Preparer

_____
Address

Dated _____ _____
Responsible Authority