MILLE LACS COUNTY EST. 1857

GUIDELINES AND PROCEDURES

MINNESOTA GOVERNMENT DATA PRACTICES ACT (MGDPA)

Table of Contents

I. INTRODUCTION

These guidelines and procedures provide assistance to Mille Lacs County staff in complying with those portions of the Minnesota Government Data Practices Act (MGDPA) that relate to access to government data and to the rights of data subjects.

The access provisions and rights are:

- The presumption is all government data is public unless classified as not public by state or federal statute or other legal authority;
- The right of any person to know what types of data are collected by Mille Lacs County about that person and how that data is classified;
- The right of any person to inspect at no charge data classified as public at reasonable times and places subject to reasonable charges that may be imposed as authorized by Minn. Stat. § 13.03, subd. 3(c), for searching for and retrieving the data;
- The right of any person to have data reasonably explained in an understandable way;
- The right of any person to get copies of government data at a reasonable cost;
- The right of any person to an appropriate and reasonably prompt response from Mille Lacs County when exercising these rights;
- The right of any person to be informed of the authority by which Mille Lacs County denies access to government data; and
- The right to be reasonably notified consistent with this policy if not public data concerning the person is subject to a breach of the security of the data.

II. OVERVIEW

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

The Act regulates:

- what data can be collected;
- who may see or get copies of the data;
- the classification of specific types of data;
- the duties of personnel in administering the Act;

- procedures for access to the data;
- procedures for classifying data as not public;
- civil and criminal penalties for violation of the Act; and
- the charging of fees for copies of data.

Government data is either data on individuals or data not on individuals. Data on individuals is classified as either public, private, or confidential. Data not on individuals is classified as public, nonpublic, or protected nonpublic. This classification system determines how data is 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 in writing by the data subject or by court order or law to see it	Nonpublic
Confidential	Not available to the public or the data subject	Protected Nonpublic

III. COLLECTION OF GOVERNMENT DATA

What is the Minnesota Government Data Practices Act?

The Minnesota Government Data Practices Act (MGDPA) is in Chapter 13 of Minnesota Statutes. It controls how government data is collected, created, stored, maintained, used and disseminated.

What is government data?

Government data is all data maintained in any form by state and local government entities. As long as data exists in some form in a government entity it is government data no matter what physical form it is in or how stored or used. Government data may be stored on paper forms/records/files, in electronic form, on audio or video tape, on charts, maps, etc. Government data may include oral statements but usually does not include mental impressions of a government official not existing in some other format.

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 county to make and keep all records necessary for a full and accurate knowledge of their official activities. Requirements for collecting, creating, maintaining, storing, and disseminating data are in Minn. Stat. 13 and Minn. Rules, Chapter 1205, the Minnesota Government Data Practices Act and Rules. Links for locating the statutes and rules are 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. Access to data that is not public shall be limited to persons whose work assignment reasonably requires access.

D. DEFINITIONS

1. Annual Report - The public document(s) required by Minn. Stat. § 13.025 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 - An individual, entity, or person authorized to act on behalf of another individual, entity or person. The authorized representative may include, but is not limited to: (a) in the case of a minor, a parent or guardian; (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 the data subject has given written informed consent for the release of the information, (e) court appointed guardian/conservator if authorized by the court order, (f) personal representative of the estate of a decedent or a decedent's heirs.

3. Court Order - The order of a judge 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 who is the subject of the data.

6. Designee - Any person designated by the 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, statewide system, or political subdivision.

8. Individual - A natural person. In the case of a minor or an individual judged by a court 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 the responsible authority shall withhold data from parents or guardians or individuals acting as parents or guardians in the absence of parents or guardians upon request by the minor if the responsible authority determines withholding the data would be in the best interest of the minor.

9. Informed Consent - The written consent given by a data subject to allow disclosure of private data about that person.

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

11. Political Subdivision - Any county, city, school district, special district, any town exercising powers under Minn. Stat. 368 and located in a metropolitan area, and any board, commission, district or authority created pursuant to law, local ordinance, or charter provision. It includes any nonprofit corporation that is a community action agency organized to qualify for public funds or any nonprofit social service agency that performs services under contract to a government entity to the extent 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 the estate of the decedent during the period of administration or if no personal representative has been appointed, or after discharge, the surviving spouse, any child of the decedent, or, if there are no surviving spouse or children, a parent of the decedent.

13. Requestor - The entity or person requesting access to and/or copies of the data.

14. Responsible Authority - Each elected official of the county is 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 offices of elected officials.

15. Rules - "The Rules Governing the Enforcement of the Minnesota Government Data Practices Act." Minn. Rules, Chap. 1205.

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 pursuant to Minn. Stat. § 13.06 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 communicated to an individual asked to supply private or confidential data concerning himself or herself and which may also be known as a Data Practices Rights Advisory.

IV. CLASSIFICATION OF GOVERNMENT DATA

For the purposes of these guidelines data is divided into four types; (a) data on individuals that is classified as either public, private, or confidential; (b) data not on individuals that is classified as either public, nonpublic, or protected nonpublic; (c) statistical or summary data derived from data on individuals

in which individuals are not identified; and (d) data on decedents. These classifications, the criteria for classification and the description of who has access are as 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) Private or confidential data may become public to comply with either a judicial order or administrative rules pertaining to the conduct of a legal action or if a statute changes or causes the classification to change. (For example: Private or confidential data that is presented in court and made public by the court.)

c. Access: All public data on individuals is accessible by all persons regardless of their interest in that data.

2. Private Data on Individuals

a. Definition: Private data on individuals is data that is not accessible to the public but is accessible to the data subject.

b. Tennessen Warning: Except for law enforcement investigations, a Tennessen Warning must be given when private or confidential data is collected from the subject of the data. A Tennessen Warning need not be given when private or confidential data is 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 data subject.

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

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

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

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

2) Individuals, entities, or persons who have been given express written permission by the data subject.

3) Personnel within the entity who have a work-related reason to access the data as determined by the responsible authority or designee.

4) 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 generally limited to the purposes for which it was originally collected.

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

6) 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) Entities or persons as otherwise provided by federal or state statutes.

3. Confidential Data on Individuals

a. Definition: Data on individuals is confidential if it is made by statute or federal law not accessible by the public and not accessible by the data subject.

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 need not be given when confidential data is collected from someone other than the subject of the data.

c. Data on Individuals is Confidential if:

1) A state or federal statute expressly provides that: (a) the data shall not be available to either the public or to the data subject, or (b) the data shall not be available to anyone except those agencies that 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 is accessible to:

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

2) Personnel within the entity who have a work-related reason to access the data as determined by the responsible authority or the designee.

3) 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) 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) Entities or persons as otherwise provided for by federal or state statutes.

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 that 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 as nonpublic or protected nonpublic is not approved by the Commissioner of Administration.

c. Access: Public data not on individuals is accessible to all persons regardless of their interest in the data.

2. Nonpublic Data Not on Individuals

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

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 data subject, 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 is accessible to:

1) The data subject, if any.

2) Personnel within the entity who have a work-related reason to access the data as determined by the responsible authority or designee.

3) Entities or persons authorized by statute or federal statute to gain access.

4) Pursuant to court order.

5) Entities or persons as otherwise provided by federal or state statutes.

3. Protected Nonpublic Data Not on Individuals

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

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, if any.

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

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

1) Personnel within the entity who have a work-related reason to access the data as determined by the responsible authority or the designee.

2) Entities or persons authorized by statute or federal law to gain access.

3) Pursuant to a court order.

4) Entities or persons as otherwise provided by federal or state statutes.

C. SUMMARY DATA

1. Definition: Summary data are statistical records and reports derived from data on individuals but in which individuals are not identified and neither their identities nor other characteristics that could uniquely identify an 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 that could uniquely identify an individual is separated from the summary data and is not available to persons who gains access to or possess summary data.

3. Access: Unless otherwise classified by a Temporary Classification, summary data is public and may be requested by and made available to any entity 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 a parent of the decedent.

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

2. Confidential Data on Decedents

a. Definition: Confidential data on decedents means data that, prior to the death of the data subject, was classified as confidential data on individuals.

b. Access: Access to and use of the data is the same as access to confidential data on individuals.

c. The representative of the decedent may exercise all rights that 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 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 to 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 30 years have elapsed from the creation of the data. For purposes of this determination an individual is presumed to be dead if either 90 years elapsed since the creation of the data or

90 years have elapsed since the individual's birth, whichever is earlier except an individual is not presumed to be dead if readily available data indicates the individual is still living.

V. REQUEST FOR GOVERNMENT DATA

No fee shall be charged for only viewing data. Pursuant to Minn. Stat. §13.03, subd. 3(c), actual costs may be required to be paid for compiling some data but not for separating public and not public data.

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. If the party requests, they shall be informed of the meaning of the data. If the data requested is public data, no form can be required, but the requestor can be asked to voluntarily complete a request and contact form. Upon request and at the discretion of the staff member, public data may be disclosed over the telephone.

Regardless of where the data originates, if it is in the possession of Mille Lacs County, it is government data and subject to the Data Practices Act, including access provisions.

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

B. REQUESTS FOR DATA ON INDIVIDUALS BY THE DATA SUBJECT

1. Upon request and when access or copies are authorized, the designee shall provide access to the private or public data on an individual to the data subject or authorized representative. See Minn. Rules, Section 1205.0500, if the data subject is a minor. If a copy is provided, the appropriate fees shall be charged unless waived consistent with county policy.

2. The designee shall respond to the request as soon as reasonably possible, and no later than ten (10) working days after receipt of the request.

3. After an individual has been shown the 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 data has been obtained about that individual.

C. REQUESTS FOR SUMMARY DATA

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

2. Within a reasonably prompt time 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 likely time schedule for preparing the requested data, including reasons for any delays and a statement of the cost, which should be pre-paid unless waived by the county; 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 the private or confidential data or is classified as other than public.

4. A non-disclosure agreement is used to protect the privacy or confidentiality of the data when the requestor of the summary data prepares the summary by accessing private or confidential data on individuals. Because of the obligation to protect the security of the data from improper access or use, such agreements will be rarely used. In the rare case of such use, a nondisclosure agreement shall contain at least the following:

a. A general description of the private or confidential data being used to prepare summary data.

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

c. A statement that the requestor understands the requestor may be subject to the civil or criminal penalty provisions of the Act for violation of the protected status of the data.

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

e. Willingness by the requestor to sign the agreement is not a guarantee of access to the data. Access may be denied if the county determines such assurances are insufficient to protect the not public nature of the data.

D. REQUESTS FOR GOVERNMENT DATA BY OTHER GOVERNMENT AGENCIES

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

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. In most circumstances, Mille Lacs County will not charge a fee to another government entity. Consideration should be given to transmission of the data by electronic means to save Mille Lacs County copying costs.

3. In many cases, data will 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, administrative, or statutory requirements such as change in classification by statutory definition. When reasonably practical, the agency providing the requested data

information shall indicate the classification of the data when the data is classified as other than public.

4. When reasonably practical and reasonably necessary, if it is not clear that the requesting agency is authorized to access the data, the requesting agency shall be directed to obtain the informed consent from the data subject(s) for data classified as private or confidential. If the agency is unable to obtain such written consent, the Mille Lacs County Responsible Authority should be consulted for a determination of access prior to release of the data.

E. HOW DATA PRACTICES APPLIES TO CONTRACTUAL LICENSING AND FUNDING RELATIONSHIP 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 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, the data are subject to the requirements of the MGDPA and the contractor must comply with the MGDPA requirements. The contract should 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 that performs services under contract to a government entity and the data is collected and used because of that contract, access to the data is regulated by the MGDPA.

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

VI. INFORMATION DISCLOSURE REQUEST FORM

A. INFORMATION DISCLOSURE REQUEST

The Information Disclosure Request 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 that occurs.

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.

VII. FEES FOR COPIES OF GOVERNMENT DATA

Pursuant to the Minnesota Government Data Practices Act and Mille Lacs County Board resolution, and unless otherwise provided for by federal law, state statute or rule, fees for copies of government data shall be determined based on the costs of providing such service as approved by the Mille Lacs County Board. Fees shall be reasonable and reflect only the actual cost.

Fees shall not be charged to those individuals who only wish to view data.

NOTE: Fees shall 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 required by statute or court order.

B. COPIES PROVIDED WITH CHARGE: When access is authorized, copies shall be provided in the following circumstances:

1. Other government agencies or responsible authorities who require or request record documents or publication copies that are not usually provided or reproduced at a cost 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 not on individuals, particularly when the requestor is not the subject of the data.

C. COPYING FEES: Copying fees shall be charged for those records, documents, and publications covered in Section B above, in accordance with Appendix A.

1. When copies are mailed, postage costs shall be added unless alternative arrangements have been made.

D. COLLECTION OF COPYING FEES: Fees shall be collected before releasing copies unless prior arrangements have been made. Payment may be required before copies are made.

VIII. 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. 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.

IX. 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 on individuals maintained by the county.

2. The public document shall be updated annually.

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

4. The county will maintain the report on its web site.

B. PROCEDURES FOR DISSEMINATION OF DATA

1. The responsible authority shall ensure 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 law.

2. Public 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 can 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.

C. DATA PROTECTION

The responsible authority shall establish procedures to assure all data on individuals is accurate, complete, and current for the purpose for which it was collected, and establish appropriate security safeguards for all data. An annual security assessment is included in this duty.

D. BREACH OF SECURITY PROTOCOL

Mille Lacs County, as required by Minn. Stat. § 13.055, has implemented a protocol in the event of a breach of security of not public data. That protocol is incorporated as an Appendix in this manual.

X. ACCESS TO GOVERNMENT DATA

A. WHO CAN MAKE A DATA REQUEST?

Anyone may seek access to data by making a data request.

B. TO WHOM MUST A DATA REQUEST BE MADE?

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

2. The responsible authority may cause preparation of summary data upon the request of any person if the request is in writing and the requestor pays in advance the cost to prepare the summary data.

3. 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 release any of the private or confidential data used to prepare the summary data; and

    b. The responsible authority determines the access will not compromise private or confidential data on individuals.

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

XI. RIGHTS OF DATA SUBJECT

A. TENNESSEN WARNING - Rights of Subjects of Data

1. Except for law enforcement investigations, every agency 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. The notice must be given whenever:

    a. A government entity requests data; and

    b. The data is requested from an individual; and

    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 must be given. These rights are referred to as the Tennessen Warning or Data Practices Rights Advisory.

    A Tennessen Warning may be given but 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. This is why the data is requested and how it will be used.

    b. Whether the individual may refuse or is legally required to supply the data. The subject has the right to know whether or not she/he is required to provide the data.

    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 may be authorized to receive the data. The notice must 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 that requests an individual to disclose their 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.

3. Tennessen Warnings may be either oral or written.

    a. Oral communication is not the preferred method of communicating the Tennessen Warning, but 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 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.

B. NOTIFICATION TO MINORS

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

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:

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

2. Whether denying access to the data may protect the minor from physical or emotional harm;

3. Whether there is a reason to believe the minor's reasons for denying access to the parent(s) are reasonably accurate; and

4. Whether the nature of the data is such that disclosing the data to the parents could lead to physical or emotional harm to the minor. Minn. Rules, Section 1205.0500, contains the procedures for the release of data about minors.

C. INFORMED CONSENT

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

   NOTE: Informed consent cannot authorize release of confidential data on individuals since the data subject has no right to the data and therefore cannot authorize another a right to access.

2. Private data shall be disseminated to any person or entity if the subject or subjects have given their valid 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 it is:

   a. In plain language;

   b. Dated;

   c. Specific in designating the particular government entity the data subject is authorizing to disclose data about the data subject;

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

   e. Specific as to the persons to whom the subject is authorizing data to be disclosed;

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

   g. Specific as to its expiration date, which must be within a reasonable period of time. 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, the consent shall not exceed two years after the date of the policy.

h. An authorization in connection with medical assistance under Minn. Stat., Chapter 256B, or MinnesotaCare under Minn. Stat., Chapter 256L, or for individual education plan health-related services provided by a school district under Minn. Stat., Section 125A.21, subd. 2, is valid during all terms of eligibility.

5. Informed consent for health insurance purposes must comply with Minn. Stat. §13.05, unless otherwise pre-empted by the HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. 164.

6. Informed consent for other purposes may be valid for longer than one year if the consent otherwise meets the above requirements.

7. 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 request is for alcohol or drug abuse patient records. It should contain the following:

    a. The name of the program that 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 the consent is signed; and

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

D. PROCEDURES FOR COMPLYING WITH DATA REQUESTS FROM AN INDIVIDUAL

The responsible authority shall ensure 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 or completeness of public or private data. If the individual notifies the responsible authority, in writing, as to the nature of the disagreement with the data, the responsible authority shall, within 30 days, either

correct the data and attempt to notify past recipients of inaccurate or incomplete 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 the data subject and specific procedures in effect in the county for access by the data subject to public or private data on individuals.

    a. When a request is denied, the responsible authority must inform the requestor orally at the time of the request, and if requested in writing as soon thereafter as reasonably possible, and shall cite the statute, temporary classification or federal law on which the determination is based.

    b. The responsible authority shall require the requestor to pay the actual costs of making and certifying copies of the data requested. The requestor may not be charged for separating private or confidential data from public data.

    c. The responsible authority shall reasonably inform the requestor of the data's meaning if asked to do so.

E. IF MILLE LACS COUNTY DETERMINES THAT CHALLENGED DATA ARE ACCURATE AND/OR COMPLETE AND THE DATA SUBJECT DISAGREES WITH THAT DETERMINATION, THE SUBJECT HAS THE RIGHT TO APPEAL THE DETERMINATION TO THE COMMISSIONER OF ADMINISTRATION

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

2. The requirements for filing an appeal are in Minn. Rules, Section 1205.1600.

3. Procedure when data is 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 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 Administrative Procedure Act, Minn. Stat. § 14.57 to 14.62 and Minn. Rules, Section

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. Stat., Chapter 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 if resolved or issue the order and notice of hearing.

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

b. After completing, correcting, or destroying successfully challenged data the county will retain a copy of the Commissioner of Administration's order issued under Minn. Stat., Chapter 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.

XII. ROLE OF THE COMMISSIONER OF ADMINISTRATION

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

B. Minn. Stat. § 13.06 gives the Commissioner certain powers with regard to approving temporary classifications of data.

C. Minn. Stat. § 13.072 gives the Commissioner authority to issue advisory opinions concerning the rights-of-data-subjects and the classification of government data. Commissioner's opinions are found at www.ipad.state.mn.us.

XIII. CONSEQUENCES FOR NOT COMPLYING WITH THE MGDPA

A. Pursuant to Minn. Stat. § 13.08, a government entity and employees may be sued for violating the Act.

B. Minn. Stat. § 13.085 provides an administrative process to compel compliance with the Act.

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

XIV. WHERE MORE INFORMATION CAN BE FOUND

A. Data Practices Compliance Official: Holly Wilson, Mille Lacs County Personnel Director/Asst County Administrator at 320-983-8378 or holly.wilson@co.mille-lacs.mn.us.

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

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

DATA REQUEST FORM - Members of the Public

Date of request:

I am requesting access to data in the following way:

☐ Inspection ☐ Copies ☐ Both Inspection and Copies

Note: Inspection is free, but there is a charge for copies. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

These are the data I am requesting:

Note: Please describe the data you are requesting as specifically as possible.

Contact Information:

Name:		
Address:		
City:	**State:**	**Zip Code:**
Phone number:	**Email:**	

Note: You do not have to provide any of the above contact information. However, if you want us to mail your requested data, we will need some type of contact information. In addition, if we do not understand your request and need to get clarification from you, without contact information, we will be unable to begin processing your request. Mille Lacs County will respond to your request as soon as reasonably possible.

(For Office Use Only)

Department/Division:	*Request handled by/Ext.:*
Method of response:	
Charges:	
Amount due:	*Received by/Ext.*

Additional Information:

DATA REQUEST FORM – Subject of Data

Date of request:

I am requesting access to data in the following way:

☐ Inspection ☐ Copies ☐ Both Inspection and Copies

Note: Inspection is free, but there is a charge for copies. If the fee for fulfilling the request is greater than $5.00, pre-payment shall be required.

These are the data I am requesting

Note: Describe the data you are requesting as specifically as possible. If you need more space, please use the back of this form.

To request data as a data subject, you must show a valid state ID, such as a driver's license, military ID, or passport as proof of identity. To request data on behalf of the data subject, you must present proper written permission granting you such access.

Data Subject Name: _____

Address: _____

Phone number: _____ Email: _____

Parent/Guardian Name (if applicable): _____

Signature of Data Subject or Parent/Guardian: _____

Mille Lacs County will respond to your request within 10 days.

(For Office use)	
ID provided:	
Department name:	***Request handled by:***
Method of response:	
Charges:	
Amount Due:	***Received by:***
Notes:	

NOTE TO DEPARTMENTS: This disclosure document is required to be used when a subject asks for data other than public data. If the request is for other than public data about another person, an informed consent authorization is also required and a copy should be kept unless specific disclosure authority otherwise exists. If disclosure is pursuant to court order, a copy of the order should be kept.

NON-DISCLOSURE AGREEMENT

1. General description of the private or confidential data that 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 liability, including but not limited to, the provisions of the Minnesota Data Practices Act in the event the private or confidential data is disclosed or used in any manner not authorized by law. See Minn. Stat. 13.08 and 13.09.

_____ _____

Requestor of Data Date

_____

Contact Information

_____ _____

Responsible Authority/Designee Date

NOTICE OF RIGHTS - TENNESSEN WARNING INSTRUCTION GUIDE

Minnesota Statutes Section 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, and used 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; • A state or federal law subsequently authorizes or requires the new use or release; or • A Court order is issued to authorize release.

"NOTICE OF RIGHTS" SAMPLE FORMAT FOR TENNESSEN WARNING

The Data Practices Act requires Mille Lacs County to inform you of your rights as they pertain to private and confidential data collected from you and about you. Some of the data we collect from you may be private data. Access to this data is available only to you, the agency collecting the data, or other statutorily authorized agencies, unless you or a court authorize its release. Some data may be classified as confidential data and is not accessible to the public or you.

The Data Practices Act requires you be advised of the following when you are asked to provide private or confidential data.

_____

The purpose and intended use of the requested data is:

_____

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

_____

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

_____

_____
Name

_____
Date

Minn. Stat. § 13.04 (subd. 2)

INFORMED CONSENT INSTRUCTION GUIDE

A. Enter the complete name and address of the entity that maintains the data. Include any relevant program names, staff names, titles and telephone numbers.

B. Identify the entity or agencies to which the data will be released. Include the name and address of the entity. Include relevant staff names and titles. Be as specific as reasonably possible.

C. Identify as specifically as reasonably possible the reports, record names, or types of data that will be released.

D. Describe specifically and completely the purpose(s) for seeking the person's informed consent.

E. Describe the known consequences, if any, of releasing the data.

F. Instruct the person to sign the consent and enter the date the consent is signed.

G. 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.

INFORMED CONSENT FOR THE RELEASE OF DATA

(see instruction guide on previous page)

I, _____ authorize
(Name of individual authorizing release)

_____ to disclose to
(A. *Name of individual, entity, or person holding record)*

_____ the following
(B. *Name of individual, entity, or person to receive the data)*

information (C.): _____

for the purpose of (D.): _____

_____

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

On specification of the date or condition upon which this consent expires:

_____

Executed this _____ day of _____ , 20 _____.

_____
*(*F. *Signature of individual authorizing release)*

_____
(Printed name)

_____
*(*G. *Signature of parent, guardian, or authorized representative, when required)*

_____
(Printed name)

DATA PRACTICES NOTICE

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

> "The data I have been requested to provide includes data classified as private or confidential data as defined by Minnesota Statute Chapter 13, the Data Practices Act. Pursuant to Minnesota Statute 13.03 and
>
> Minnesota Rules, Section 1205.0100, Subd, 5, the Court's attention is called to this classification. The Data Practices Act provides 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 data, I will do so."

APPENDIX A
FEE SCHEDULE
FOR FAXING AND PHOTOCOPYING

(COUNTY AND NON-COUNTY MATERIALS)

(Sales tax exempt)

Photocopies/Printer Copies:	$ .25 per page, up to 100 standard pages For copies in excess of 100 pages of letter or legal sized black and white documents, actual charges may be required if they exceed the per page charge – Minnesota Statute13.03, subd. 3(c).
Postage and Handling:	Actual cost

APPENDIX B
MGDPA, CHAPTER 13

https://www.revisor.mn.gov/statutes/?id=13

APPENDIX C
MGDPA, CHAPTER 1205

State of Minnesota

Department of Administration

Data Privacy Division

To read a copy of this section, please go to the following website:

https://www.revisor.mn.gov/rules/?id=1205

APPENDIX D

Mille Lacs County - Responsible Authorities

Department	Responsible Authority	Designee
Administration	County Administrator	Holly Wilson
Assessor	County Administrator	Al Heim
Attorney	Joe Walsh	Heather Griesert
Auditor/Treasurer	County Administrator	Philip Thompson
Community and Veterans Services	County Administrator	Beth Crook
Court Administration	Cheryl Woehler	
Land Services	County Administrator	Michele McPherson
Probation Office	Ben Davis	
Public Works	County Administrator	Bruce Cochran
Sheriff	Brent Lindgren	Kent Larson
U of M - Extension	County Administrator	

County Data Practices Compliance Officer: *Holly Wilson, Personnel Director/Asst County Administrator*

APPENDIX E
DATA SECURITY BREACH PROTOCOL

Part 1. Purpose.

This protocol is intended to assist Mille Lacs County in implementing the requirements of Minn. Stat. § 13.055 that is intended to provide timely and appropriate notice to individuals who are affected by a breach of the security of their private or confidential data. All employees must immediately report known or potential breaches of security to the responsible authority and their supervisor. The County Attorney's Office, in consultation with the affected department or office, shall determine whether notice of the potential breach is required and, if so, how the notice will be provided.

Part 2. Definitions. Minn. Stat. 13.055, Subd. 1 (in part)

Subpart A. Potential Data Security Breach. A situation or incident that provides a reasonable basis to believe not public data may have been compromised or accessed for a purpose not authorized by law, or by a person or entity not authorized by law to have access to such data.

Subpart B. Breach of the security of the data. Breach of the security of the data means the unauthorized acquisition of data maintained by the county in any medium that compromises the security and classification of the data, but not including the good faith acquisition by an employee, contractor, or agent of the county, if not provided to an unauthorized person.

Subpart C. Contact Information. Contact information means both name and mailing address, or name and e-mail address for each individual who is the subject of data maintained by the county.

Subpart D. Unauthorized acquisition. Unauthorized acquisition means a person has obtained government data without the informed consent of the individuals who are the subjects of the data, or lacks statutory or other legal authority and with the intent to use the data for non-governmental purposes.

Subpart E. Unauthorized person. Unauthorized person means any person who accesses government data without permission or without a work assignment that reasonably requires the person to have access to the data.

Part 3. Guidelines

Subpart A. Reporting a Potential Breach. Any employee who knows of or reasonably believes breach of the security of private or confidential data may have occurred must immediately report to his or her supervisor and the county's responsible authority (R.A.).

The report should include the date and time of the report, when the breach occurred (if known); the type of data involved; the approximate number of affected individuals, if known, and other pertinent data. The attached form should be used for that purpose whenever reasonably possible.

Employees who, in good faith, report a potential or actual breach under these guidelines will not be subject to retaliation for making such a report.

Subpart B. Breach Affected Division Response Process. After a potential breach of security has been reported, the responsible authority will work with the affected department or office to take necessary steps to contain and control the integrity of the data handling systems impacted by the potential or reported breach and conduct a preliminary internal assessment of the scope of the potential breach. Applicable staff and security procedures or other guidelines may be consulted as set forth in this policy.

If the potential breach is on a county computing system that contains or has network access to private or confidential data, the R.A. shall consult with IT personnel and consider control measures that may include but are not necessarily limited to removing the computing system from the network.

a) Determining Breach. The responsible authority shall consult with the affected staff supervisor to determine whether a breach of security of data has occurred.

b) Incidents. Examples of the types of incidents that may result in a notice triggering breach include, but are not limited to:
   i. Evidence of unauthorized access into a computer system containing private/confidential data;
   ii. Missing documents or papers or stolen or missing laptop, desktop, storage device or other types of information technology resource containing files with private/confidential data;
   iii. Documents containing private/confidential data sent in any form to a wrong recipient;
   iv. IT Systems containing private/confidential data that has been compromised; or
   v. Employee misuse of authorized access to, or disclose of, private or confidential data.

c) Acquisitions. Minn. Stat., Sect. 13.055, subd. 2, requires government entities to notify individuals if their private or confidential data has been, or is reasonably believed to have been, acquired by an unauthorized person. In making that determination, the following factors, among others, may be considered:
   i. Indications that the data is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device or documents containing unprotected private or confidential data.
   ii. Indications that the data has been downloaded or otherwise acquired.
   iii. Indications that the data was used by an unauthorized person such as a fraudulent account opened or an instance of identity theft reported;
   iv. The encryption protection of the data, if any;
   v. Duration of exposure;
   vi. The extent to which the compromise of electronic data indicates a directed attack such as a pattern showing that the device itself was specifically targeted; or
   vii. Indications that the attack was intended to seek and collect private or confidential data.

1. Timing of Notification. If a breach has been determined, in most instances, the affected department or office has primary responsibility to notify affected individuals and may be assisted by the R.A. Notice is to occur without unreasonable delay. Notice may be delayed due to a) the legitimate needs of a law enforcement agency; or b) any measures necessary to determine the scope of the breach and restore the reasonable security of the data.

Immediate notification may be appropriate in the event of a breach that could have immediate deleterious impact on individuals whose data may have been acquired by an unauthorized person.

2. Contacting Law Enforcement. The responsible authority or designee(s) shall contact law enforcement agencies if the breach of security is believed to involve illegal activities. Data may be shared with law enforcement consistent with applicable data practice laws. If law enforcement is contacted, it should be informed of the County's practice to provide notice to affected individuals. If law enforcement advises such notice would impede an active criminal investigation, notice may be delayed. Delayed notice should be sent out as soon as law enforcement advises it would no longer impede the criminal investigation.

3. Whom to Notify. The responsible authority, in consultation with other appropriate county personnel, including but not limited to the affected department or office, shall determine the scope of the notice. Notice of a breach must be provided to any individual whose private or confidential data has been or is reasonably believed to have been acquired by an unauthorized person. If specific individuals cannot be identified, notice should be sent to groups of individuals likely to have been affected, such as all whose data is stored in the database of files involved in the breach. Measures should be taken to prevent notice lists from being over-inclusive. If questions arise regarding the scope of the notice required, the County Attorneys' Office may be contacted for guidance.

Subpart C. Notice.

1. Content. The responsible authority or designee shall consult with the affected department or office on the wording of a notice. Notices shall generally be sent separate from other documents. The notice should use clear and plain language.

   The following should generally be included in the notice:

   a) A general description of what happened and when, to the extent known.

   b) The nature of the individual's private or confidential data that was involved, but not listing the specific private/confidential data.

   c) Information about what the county has done to protect the individual's private/confidential data from further disclosure.

   d) Institution assistance, such as website information or telephone number, for further information about the incident.

   e) Information, such as Web sites, about what individuals can do to protect themselves against identity theft, including contact information for nationwide credit reporting agencies.

2. Method of Notification. The responsible authority, in consultation with the affected division, shall determine the appropriate method of notice as follows.

   a) Written notice by first class mail to each affected individual; or

b) Electronic notice to each affected individual if communication normally occurs in that medium and the procedure is otherwise consistent with the provisions regarding electronic records and signatures contained in 15 U.S.C. 7001.

c) Substitute notice may be provided if the cost of providing the written notice required to each affected individual would exceed $250,000 or the affected class of individuals to be notified exceeds 500,000 or the county does not have sufficient contact information to notify affected individuals. Substitute notice consists of all the following:

i. E-mail notice if the county has an e-mail address for the affected individuals;

ii. Conspicuous posting of the notice on the county website for a minimum of 45 days and

iii. Notification to major media outlets that reach the general public.

Subpart D. Coordination with Credit Reporting Agencies. Credit reporting agencies assist individuals in responding to a notice of a security breach. Such agencies should be notified in advance of sending notice of security breach incidents that may significantly increase calls to agencies for assistance.

If notice is required to be given to 1,000 or more individuals at one time, the county shall notify without unreasonable delay all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis as defined in 15 U.S.C. 1681a, of the timing, distribution and content of the notice to be sent. Such contacts shall include but not be limited to the following:

- Equifax:
  U.S. Consumer Services
  Equifax Information Services, LLC.
  Phone: 1-800-525-6285

- Experian:
  Experian Security Assistance
  P.O. Box 72
  Allen, TX 75013
  Phone: 1-888-397-3742

- TransUnion:
  Phone: 1-800-680-7289

Subpart E. Documentation. The responsible authority or designee must complete a Breach of Security Incident Response Summary for each reported breach, regardless of whether notice is given. The form should be completed beginning at the time of the initial report, or as soon thereafter as reasonably practical.

Where appropriate, all documentation related to the breach and investigation shall be labeled and maintained as not public pursuant to the applicable data privacy classification, including but not limited to, “security information”, as defined by Minn. Stat. 13.37, Subd. 1(a). The form shall be retained by the responsible authority in accordance with the applicable records retention policy.

Potential Not Public Data Breach Report

Name of Reporting Person(s): _____

Department or Office: _____

Division: _____

Email: _____

Telephone Number: _____

Date of Report: _____

Time of Report: _____

Date and Time of Discovery of Potential Breach: _____

_____

To Extent Known Date and Time of Potential Breach: _____

_____

Type of Data Involved: _____

_____

Method of Breach to Extent Known or Suspected: _____

_____

Number of Affected Persons: _____

_____

Additional Comments: _____

_____

_____

_____

Signature of Reporting Person

This report must be promptly completed and forwarded to Joe Walsh, Mille Lacs County Attorney. It may be emailed to joe.walsh@co.mille-lacs.mn.us.

For any assistance or questions, call 320-983-8305