Meeker-McLeod-Sibley Community Health Services

Data Practices Policy

Mission

Lead efforts to protect and promote the health of the people in Meeker-McLeod-Sibley counties through education, empowerment and provision of essential public health services.

Public Health
Prevent. Promote. Protect.

Meeker McLeod Sibley
Community Health Services

Table of Contents

Meeker-McLeod-Sibley Community Health Services Data Practices was approved and adopted on April 9th, 2015.

Ron Shimanski

Meeker-McLeod-Sibley Community Health Board, Chair 2015

This document will be reviewed annually at a MMS CHS Board Meeting.

Reviewed:

Date	Reviewed	Staff Initial	CHB approved	Board Chair Signature

BRIEF OVERVIEW OF THE MINNESOTA GOVERNMENT DATA PRACTICES ACT

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

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 by 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 present 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. CH. 13 AND MINN. R. 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.

Definitions

Authorized Personnel—Any CHS staff including full- or part-time employees, contractors, and federal assignees that require access to confidential information to conduct their duties. Other persons may also be authorized access to confidential information as described below.

Confidentiality—The obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for, and to protect and preserve, the privacy of others.

External Report—Any report written by CHS staff that will be shared with an outside agency or person.

Other Authorized Persons—Other persons who are not CHS employees (e.g., trainees, students, volunteers, interns, etc.) may under certain circumstances be authorized to

access confidential information for a specific project or purpose. All requests for such persons to be authorized must be approved by the CHS Director.

Program Manager—Program Managers are employees who report directly to the CHS Director and are responsible for overseeing one or more of the Section's programs.

Secondary Data—Data that have been collected by an agency other than the CHS and provided to the CHS for use are considered secondary data. Examples of secondary data include population census data, vital statistics data, and school enrollment data. Secondary data may or may not contain confidential information.

Summary Data—Data provided by the CHS may include summary information grouped by age, sex, or geographic area and displayed so that individual clients, physicians or institutions are not identifiable.

Confidentiality Policies and Procedures

Confidentiality procedures in the Meeker McLeod Sibley Community Health Service (MMS CHS) are intended to protect the privacy of clients and the facilities reporting these clients to the CHS, to ensure the integrity of data, and to comply with confidentiality-protecting legislation and administrative rules. All Programs within the CHS must adhere to these policies and procedures; additional more stringent policies may be developed by individual Programs that are tailored to their specific needs.

Responsibility to Safeguard Confidentiality

All data including but limited to, client, agency, program or surveillance data is kept confidential according to appropriate statute, rules or regulations per this policy. Every person working in the Meeker McLeod Sibley Community Health Service (MMS CHS) has an ethical and legal obligation to protect the privacy of the persons whose records the CHS maintains.

1. Personal Identifiers—No information which identifies a specific individual, health care provider, or hospital is to be shared with anyone except as delineated by these policies and procedures. If an outside agency, institution or individual (e.g., news media) possesses confidential information, CHS staff will neither confirm nor deny the accuracy of the confidential information held outside the CHS. The obligation to protect confidential information extends indefinitely, even after the death of the client or termination of employment in the CHS.

2. Data Security and Confidentiality Trainings—All staff with access to data that contains PHI will be required to review a copy of this policy and have an opportunity to ask questions and have them answered. An annual CHS data

security and confidentiality training will be offered online for staff to complete found at https://data-securitytraining.dhs.mn.gov/ .

3. Requirements for Contractors and Grantees—Appropriate language reflecting the CHS confidentiality policy and practices must be incorporated into all contracts and grants awarded by CHS for which there will be sharing of PHI by the recipient. These additions should include information about how to report breaches and potential consequences.

Release of Summary Public Health Data in Reports

Published data, e.g., data published in an executive summary or as a fact sheet that was previously publicly available, can be released by any CHS employee. Release of data or reports that were previously available to a limited group of stakeholders should be considered on a case-by-case basis in consultation with the Program Manager and the CHS Director. CHS staff is required to obtain review by Program Managers of all reports to be released externally to ensure that confidentiality has been maintained.

Summary Data Release Protocol

The purpose of this protocol is to protect the confidentiality of client information when the CHS releases public health data to external stakeholders. Summary data are information grouped by age, sex, geographic area, or other variables and displayed so that individual clients cannot be directly identified. Summary data may be presented as a table, figure, diagram, chart, narrative, line list, or other similar format. Examples of summary data are the annual infectious disease reports and the sexually-transmitted disease summaries routinely published in the fact sheets . Summary data also may be produced on an ad hoc basis for various agencies and entities upon request.

Although summary data do not include confidential data such as a client's name, summary data may lead to de facto identification of a particular person if the combination of age, sex, place of residence, or other variable(s) defines only one person — this is particularly important for communities with a relatively small population. Both numerators and denominators should be considered when releasing data; it is never acceptable to release summary data that could reasonably be expected to lead to the identification of an individual client through indirect means. Because of this potential for a breach of confidentiality, great caution must be exercised in the distribution and use of such data.

Before summary data are released, CHS program managers must carefully review and approve the data format to ensure that the release is consistent with the guidelines in this protocol. If there is a question as to whether the release is consistent with the

guidelines in this protocol, program managers should consult with the CHS Director prior to granting approval. In some circumstances, the guidelines might not be sufficiently restrictive to prevent identification of individuals because of the distribution of the health condition or the population affected. In those instances, parameters more restrictive than the general guidelines should be instituted before data can be released. Program Managers are responsible for maintaining records of data requests and subsequent data releases.

PROCEDURES FOR DISSEMINATION OF DATA

1. The CHS Director shall ensure each team 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. 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 CHS Director.

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

    c) The additional use has been approved by the CHS Director 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.

Release of Secondary Data

Except as pertaining to MIIC, Minnesota's immunization information system, CHS does not release original, individual-level data that were collected by another agency and then reported to CHS. Persons requesting data from CHS that did not originate in CHS should be referred to the agency or institution with primary responsibility for collecting the data.

Release of Confidential Data to Health Care Providers, Health Officials, and Clients

Staff must protect the identity of clients while working with external organizations. In some instances, non-confidential information may be used to identify individual clients or institutions through indirect means (e.g., combinations of variables might be enough

to specifically identify an individual living in a small community). Great caution must be exercised in the use of such data because of the potential to breach confidentiality. The following guidelines apply to the release of confidential CHS data to hospitals, health care providers, and other state or federal agencies that provide or oversee direct health-care services.

1. Release of Data to Hospitals, Health Care Providers, Public Health Officials and Clients- Release of confidential data to Hospitals, Health Care Providers, Public Health Officials and Clients will only be done when an appropriate consent form is signed,

2. Releases and Requests Specific to an Immunization Information System—The intent of the Minnesota Immunization Information System , i.e., MIIC in Minnesota, is to collate immunization data for individuals and allow access to that information by authorized health care providers and clients, and other entities covered under permitted disclosures. Agreements and policies covering these specific incidences should be referred to the Minnesota Immunization Program Manager.

Transmission of Confidential Data

Authorized CHS staff may transmit confidential information if they have followed all the previous protocols and do the following:

1. *Transmission via Telephone*—When transmitting confidential information by telephone, staff members must:

    - Verify the identity of all requestors seeking the disclosure of confidential information over the telephone by obtaining a written request for data if the party or agency is unknown to CHS staff members.

    - Whether using landlines, cellular telephones, or public telephones, disclose confidential information by telephone only from a secure or private area.

    - Never leave messages with confidential information on voicemail, answering machines or with individuals other than the data subject or their personal representative unless the voicemail/answering system is known to be protected (e.g., that of a public health nurse). Information left in messages shall be generic in nature and not indicate the services being performed or the provider of such services, unless the data subject has directly requested otherwise and this is documented

in the data subject's record. An example of a generic message is, "My name is Jenny Smith. Please return my call at 867-5309."

2. *Transmission via Mail*—When sending confidential information by U.S. mail, CHS staff must:

    - Verify that the correct confidential information is being mailed to the correct individual(s);
    - Send the information in a security envelope marked "Confidential;"
    - Include the sender's name and a return address;
    - To the extent possible, verify that the recipient's address is correct; and
    - Whenever feasible, send the information by registered or certified mail, or another method that provides delivery tracking.

3. *Transmission via Delivery or Courier Service*—When sending confidential information by hand delivery or courier service, CHS staff must:

    - Verify that the correct confidential information is being delivered to the correct individual(s);
    - Verify the name and address of the intended recipient;
    - Seal the information under protective cover (e.g., a folder or envelope) and mark the package "Confidential;"
    - Use a reputable courier service known to the Division;
    - Request identification from the courier, record the courier's name and time of pick-up; and
    - If possible, retain a tracking number so that in the event the intended recipient informs you that the package was not received, you are able to track the item with the delivery service.

4. *Transmission via Facsimile (Fax)*—When sending confidential information by facsimile machine, staff members must:

    - Verify the fax number of the intended recipient;
    - Aside from faxes to routine/known recipients (e.g., public health offices, health care providers), telephone the recipient to alert him/her that a fax containing confidential information is to be transmitted;

- Transmit the fax using a CHS-specific cover sheet that contains a confidentiality statement and instructions directing the unauthorized recipient of a misdirected fax to contact the sender. In the event of a misdirected fax, the unauthorized recipient should be directed to immediately destroy the fax or return the information to the sender, as directed by the sender.

- For faxes to non-routine recipients, if the recipient does not confirm receipt within a reasonable period of time, call the recipient to confirm receipt.

- Remove the faxed documents from the vicinity of the fax machine, including the fax activity confirmation sheet after transmission. Keep fax activity confirmation sheets with original documents.

- Locate fax machines in a secure, lockable area to which only authorized CHS staff have access.

5. *Transmission via Electronic Mail (E-mail*)—Standard electronic mail must not be used directly to send or receive confidential data, regardless of whether an email is sent to an outside party or to another CHS staff member.

   However, as approved by the Department, selected software products that can encrypt messages (such as Direct Securing Messaging) are acceptable for transferring PHI or additional protected information. Program Managers must ensure that staff are aware of and adhere to the Department policies governing the use of encryption products. Program Managers will work with staff to request outside agencies who communicate confidential information to CHS not to include any identifying information on electronic mail messages. Other agencies may have their own encryption software for electronic mail (e.g. Prime West, South Country Health Alliance, Health Insurance Providers); check with the CHS Director about whether that use is acceptable on a case-by-case basis.

6. *Transmission via Scanner*—Hard copy data that contains PHI may sometimes need to be transformed to an electronic format to be saved or archived. The CHS policy is to temporarily assume the risk involved with scanning a document and delivering it to a state email address. However, CHS policy is more restrictive in that all documents with PHI should be scanned only to a secure encrypted jump drive and then saved to a secure network location or attached to an e-mail using previously described secure methods (see #5 above).

7. *Exemption for Transmission of Employment Records*—Employment records held by a covered entity in its role as employer may be transmitted electronically via e-mail or scanner.

PROCEDURES FOR COMPLYING WITH DATA REQUESTS FROM AN INDIVIDUAL

The CHS Director shall ensure each team establishes procedures to comply with requests for government data in an appropriate and prompt manner.

1. Upon request to the CHS 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 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 except those exempt. 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.

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. Rule 1205.0500 contains the procedures for the release of data about minors.

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's right to access.

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.
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, this must be within a reasonable period of time. In the case of authorizations given in connection with applications for life insurance or noncancellable 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 chapter 256B or MinnesotaCare under chapter 256L, or for individual education plan health-related services provided by a school district under section 125A.21, subdivision 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 HIPPA 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 client records may be made only if the consent is in writing and expressly states the request is for alcohol or drug abuse client 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 client;

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 client and, when required, of a person authorized to give consent.

8. A sample format is on page 23 of this manual.

On-Site Security

All CHS employees are responsible for data security. There are many aspects to securing data and it is critical to have several levels of data security to ensure the confidentiality of clients as well as to ensure data integrity.

1. *Workstation Security*—To minimize the opportunity for CHS staff or worksite visitors to inadvertently view confidential health information to which they should not have access, CHS staff shall adhere to the following guidelines at all times:

    - Workstations at which confidential data are handled are to be located in secure areas of CHS or Department property.

    - Computer monitors should be turned so that they are not facing hallways or other heavily trafficked areas. If a monitor must be placed facing the hallway, a security screen should be used.

    - When creating passwords, best practices and guidelines from individual County IT Deparnts will be followed.

    - Passwords must not be shared.

    - No one should use a computer while it is operating under another person's password.

    - Passwords should not be displayed in the work area.

    - Documents containing confidential information should be turned face-down when the workstation is unattended during work hours; these

documents should be stored in a locked file cabinet before leaving the workspace at the end of the day.

- CHS staff must log off or lock their computers when stepping away from their desks for an extended period or leaving at the end of the day.

- Work should not be saved to individual computer hard drives but rather to shared secured network drives.

2. *Office Access*—The main CHS office (McLeod County Glencoe Building) is secured with outer doors with suitable locks to prevent access by unauthorized personnel. During the work day, public entrance to CHS is limited to access only through McLeod County Social Services Main Entrance; other hallway doors will be secured at all times. MMS CHS will follow McLeod County Public Health Security Procedures.

3. *Internal Access to Offices*—Program Managers or their designees are responsible to ensure the security of staff work areas. When not in use by authorized personnel, program offices where confidential data are stored will be locked. Keyed office access will be limited to those individuals designated by the Program Managers.

4. Paper-Based Confidential Information—CHS staff must properly store on-site paper-based files as follows:

    - Store paper-based confidential information in a locked file cabinet;

    - Position file cabinets or other storage sites away from public areas, preferably in low-traffic areas, and if possible closest to staff who will be regularly accessing the data stored within;

    - Store file cabinets without locks in rooms that can be locked or otherwise secured; limit access to rooms with unlocked cabinets based on need–to-know, role-based access.

    - Staff should immediately retrieve papers that contain confidential information from printers and copy machines.

5. *Electronic Confidential Information*—Electronic confidential information shall be maintained by the data custodian in a manner that protects the confidentiality, integrity, and availability of the information.

- A computer from which confidential information is accessed must be password-protected and configured to adhere to the current CHS standard of encryption technology.
- Confidential information stored on any removable media (e.g., thumb drives) must be saved using encryption technology that meets CHS standards.
- Confidential information stored on any portable devices (e.g., laptops) must be saved using encryption technology that meets CHS standards.
- Program Managers should ensure that staff members have been trained on the appropriate use of the various CHS network drives.
- Workforce members shall not circumvent prescribed access rights by sharing their passwords or utilizing another workforce member's password to access confidential information beyond the scope of their authority.

6. *Records Retention*—Records, whether electronic or in hard copy, must be retained per the CHS's Records Retention Schedule that was last updated in 2013.

7. *Changes to Employment Status*—When an CHS staff member resigns, retires, is terminated or transferred, CHS administrative staff must ensure that the appropriate steps have been taken to restrict future access of the non-employee to CHS offices. MMS CHS will follow McLeod County's policies for employees' status changes. This includes:

    - The individual passcodes to locked doors are inactivated centrally; and
    - Individual county Information Technology staff (IT) are immediately notified to immediately terminate former employees rights and access.

Off-Site Security

CHS staff shall not remove confidential information, including paper or electronic information, from the work site unless it is required for a field visit, meeting, or otherwise necessary for work-related purposes and only if authorized by a member of the CHS Management Team. Appropriate measures shall be taken in each instance to ensure that confidential information removed from the worksite is secured from unauthorized access and not left unattended in an unsecured area or container.

1. *Data Collection Using Portable Computers*—Laptop computers, PDAs, and other portable devices on which confidential information is stored should be protected

at all times and should not be left unattended. While in automobiles, laptops, PDAs, and other portable devices should be kept out of sight (e.g, in a trunk or hidden under a seat) and locked when the car is unattended. Laptops, PDAs, and other portable devices on which confidential information is stored should not be loaned to any unauthorized person, including family members.

CHS staff may collect data in the field onto a CHS-issued laptop (portable) computer outfitted with appropriate encryption software. Each staff member will be responsible for securing the data collected to prevent access by unauthorized personnel. If air travel is involved, laptop computers, PDAs, and other portable electronic devices will be handled as carry-on luggage. When not in use, the computer, PDAs, and other portable devices will be kept in a secure area. PHI data should not be viewed on laptops or other devices when the screens cannot be secured in a public space, e.g., while working on an airplane.

Upon returning from the field, staff will bring the portable computers and any backup portable storage devices to the CHS office and data will be transferred to the employee's desktop computer and stored on a secure hard drive. PHI data will then be permanently deleted from the portable computers and any backup portable storage devices. Alternatively, the backup portable storage devices may be secured (locked) in an archive files and retained according to the State retention schedule.

2. *Data Collection [Using Other Methods]*—When CHS staff collect data in the field that are hard copies in the form of medical records, forms, handwritten abstracts or other paper materials, these data will be secured by each individual staff member to prevent access by unauthorized personnel. If air travel is involved, the case will be handled as carry-on luggage. When not in the staff member's possession, it will be kept in a secure area. Hard copy data should not be left unattended in automobiles. Upon returning from the field, staff will bring the hard copy data to the CHS office and secure it in a locked filing cabinet until the collected data can be transferred to another media. All hard copy data will be retained according to the State retention schedule.

3. *Off-Site Data Storage of Electronic Data Files*—confidential electronic data stored in an off-site facility must be transported and stored according to current CHS IT security standards.

4. *Alternate Work-Sites*—In the event of an emergency, CHS may need to relocate staff and computers to an alternate work site location. Temporary work stations will be set-up according to CHS IT security standards. The general principles of measures to protect the confidentiality of data will be in effect, although may need to be adapted to the current circumstances, i.e., no locking offices, therefore records may need to be stored in locking portable filing cabinets.

Disposal of Confidential Data

Confidential data that are no longer needed shall be destroyed or archived, in accordance with the CHS's record retention and disposal policies. Data will be destroyed as follows:

- Hard copy data will be shredded on-site prior to disposal.
- Confidential data stored on fixed and removable electronic media must be destroyed so that it cannot practicably be read or reconstructed. Data destruction techniques and procedures are made official by the CHSS Security Officer.
- Only after the above steps have occurred will material be placed in general office waste.

APPENDIX A

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.

APPENDIX B

"NOTICE OF RIGHTS"
SAMPLE FORMAT FOR TENNESSEN WARNING

The Data Practices Act requires Washington County to inform you of your rights as they pertain to private and confidential data collected from you and about you. Some of the personal 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 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)

APPENDIX C

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

C. 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.

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. Instructions for completing this portion of the form within your particular entity should be developed in consultation with the County Attorney's office.

APPENDIX D
SAMPLE OF AN INFORMED CONSENT FOR THE RELEASE OF DATA

I,_____
(Name of individual authorizing release)

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

to disclose to_____
(Name of individual, entity, or person to receive the data)

the following information:

_____

for the purpose of:

_____
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_____.

_____
(Signature of individual authorizing release)

_____
(Printed name)

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

APPENDIX E

MINNESOTA GOVERNMENT DATA PRACTICES ACT

CHAPTER 13

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

(Click on "Retrieve an Entire Chapter". In Chapter Box type "13". Then, check on "Get Chapter")

APPENDIX F

MINNESOTA GOVERNMENT DATA PRACTICES ACT

CHAPTER 1205

State of Minnesota
Department of Administration
Data Privacy Division

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

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