New Employee Orientation

Data Practices

MDH Minnesota Department of Health

CHS Administration Handbook

Rev. 2013

http://www.health.state.mn.us/divs/opi/gov/chsadmin/data/mgdpa.html

What is the Minnesota Government Data Practices Act?

The Minnesota Government Data Practices Act (MGDPA), Minn. Stat. § 13, is a state law that controls how government data are collected, created, stored (maintained), used and released (disseminated). The MGDPA sets out certain requirements relating to the right of the public to access government data and the rights of individuals who are the subjects of government data.

Briefly, the MGDPA regulates:

- What information can be collected
- Who may see or have the information
- Classification of specific types of government data
- Duties of government personnel in administering the provisions of the MGDPA
- Procedures for access to the information
- Procedures for classifying information
- Civil penalties for violation of the MGDPA
- Charging fees for copies of government data

The actual text of Minn. Stat. § 13, and Minn. R. 1205, the Rules Governing Data Practices as promulgated by the Minnesota Department of Administration, can be found online.

What are Government Data?

Government data is defined as "all data collected, created, received, maintained, or disseminated by any government entity regardless of its physical form, storage media, or conditions of use." Thus, as long as information is recorded or stored in some way by a government entity, they are government data, no matter what physical form they are in, or how they are stored or used. Government data may be stored on paper, in electronic form, on audio or videotape, on charts, maps, etc. Government data does not include mental impressions.

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

Who must comply with the MGDPA?

The MGDPA applies to all data collected, created, received, maintained or disseminated by any government entity. The MGDPA defines "government entity" as "a State agency, statewide system, or political subdivision." The term "political subdivision," for purposes of the MGDPA, includes counties, cities, school districts, special districts, boards, commissions, and district; as well as authorities created by law, local ordinance or charter provision. State-level entities include the University of Minnesota and state-level offices, departments, commissions, officers, bureaus, divisions, boards, authorities, districts, and agencies.

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

Additionally, if a government entity enters a contractual arrangement with a private party to perform any governmental function, that private party is subject to the MGDPA with regards to any of the data created, collected, received, stored, used, maintained or disseminated in the performance of the agreement and must comply with the MGDPA as if it were a government entity.

What are the consequences for MGDPA noncompliance?

A government entity may be sued for violating any MGDPA provisions. An action to compel a government entity to comply with the MGDPA may be brought in either a Minnesota District Court or with the Minnesota Office of Administrative Hearings. A government entity found to be in violation may be ordered to comply with the MGDPA, pay a civil penalty up to $1,000, and pay the aggrieved person's costs and disbursements including attorney's fees. Additionally, the MGDPA provides criminal penalties, and disciplinary action including dismissal from public employment, for anyone who willfully (knowingly) violates a provision of the MGDPA.

Where can more information about the MGDPA be found?

The following sources may provide helpful information about the MGDPA and other data practices laws.

Local government associations may be consulted for information specific to data practices matters within their jurisdiction.

- Association of Minnesota Counties
- Minnesota County Intergovernmental Trust
- League of Minnesota Cities
- Minnesota School Boards Association
- Minnesota Association of County Officers
- Minnesota Police and Peace Officers Association

Additionally, information, educational resources, and assistance with data practices issues are available from the Minnesota Department of Administration Information Policy Analysis Division (IPAD).

Opinions issued by the Commissioner of Administration, pursuant to Minn. Stat. §13.072, are available on the IPAD website. Copies of individual opinions, an opinion summary, and an index to Commissioner's Opinions are available from IPAD upon request.

Definitions and Classifications of Data

The MGDPA establishes a system of data classifications that define, in general terms, who is legally authorized to access government data. This classification system is constructed from the definitions provided in Minn. Stat. §13.02. See also: Minn. R. 1205.0200.

Almost all government data are either data on individuals or data not on individuals. The MGDPA defines an "individual" as a natural person, and, in the case of a minor or incapacitated person, a parent or guardian. Thus, other legal entities such as corporations are not considered an "individual" for purposes of the MGDPA. "Data on individuals" is all government data in which any individual is or can be identified as the subject of that data. Data on individuals are classified as public, private, or confidential. In contrast, "Data not on individuals" is all government data which is not data on individuals, and are classified as public, nonpublic, or protected nonpublic. This classification system determines how government data are handled.

Public Data

Public data is accessible by anyone. The MGDPA provides that, unless specifically authorized by statute, a government entity may not require persons to identify themselves, state a reason for, or justify a request to gain access to public government data.

Private Data

Private data on individuals is data classified by statute or federal law as not public but accessible to the individual subject of that data.

Confidential Data

Confidential data on individuals is data made not public by statute or federal law and is inaccessible to the subject of that data.

Nonpublic Data

Nonpublic data is data not on individuals that a statute or federal law makes not accessible to the public but accessible to any subject of that data.

Protected Nonpublic Data

Protected nonpublic data is data not on individuals which is both not public and not accessible to the subject of that data.

The MGDPA specifies that all government data is public unless a statute, a temporary classification issued by the Commissioner of Administration, or a federal law classifies the data as, with respect to data on individuals, private or confidential; or, in the case of data not on individuals, as nonpublic or protected nonpublic. In this regard:

Data on Individuals	Data on Decedents	Data Not on Individuals
Public (Minn. Stat § 13.02, subd. 5) Accessible to anyone for any or no reason	**Public** (Minn. Stat. § 13.10, subd. 1) Accessible to anyone for any or no reason	**Public** (Minn. Stat § 13.02, subd. 4) Accessible to anyone for any or no reason
Private (Minn. Stat § 13.02, subd. 12) Accessible to data subject; not available to public	**Private*** (Minn. Stat. § 13.10, subd. 1b) Accessible to representative of decedent; not accessible to public	**Nonpublic** (Minn. Stat § 13.02, subd. 9) Accessible to subject of the data, if any; not accessible to public
Confidential (Minn. Stat § 13.02, subd. 3) Not accessible to data subject; not accessible to public	**Confidential*** (Minn. Stat. § 13.10, subd. 1a) Not accessible to representative of decedent; not accessible to public	**Protected Nonpublic** (Minn. Stat § 13.02, subd. 13) Not accessible to data subject; not accessible to public

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

Collecting and Storing Data

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

Related Chapter

Government Records and Retention

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

Before the Minnesota legislature ended its 2012-2013 session, it passed a bill that revises the Minnesota Data Practices Act to classify "individual personal e-mail addresses and telephone

numbers collected by government entities for notification purposes as private data on individuals and allowing data sharing among government entities."

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

- Identify its specific legal authority(ies) for collecting, using, disseminating, and storing public, private, or confidential data on individuals.
- Determine what types of data on individuals it collects or stores, and how those data are classified.
- Designate a "Responsible Authority," who is the individual ultimately responsible for the collection, use, and dissemination of government data.
- Pursuant to Minn. Stat. §13.05, subd. 1, prepare a public document containing, among other information, a description of each category of record, file, or process relating to private or confidential data on individuals maintained by that entity. This public document must contain the name, title, and address of the entity's responsible authority. Forms that are used by the entity to collect private and confidential data on individuals must be included in the document. The document must be updated annually. Entities are not required to prepare a public document for data not on individuals.

Tennessen Warnings

Whenever a government entity asks an individual to provide private or confidential data about her/himself, the entity must give that individual a notice—sometimes called a Tennessen warning.

What must be included in the notice?

Pursuant to Minn. Stat. §13.04, subd. 1, an individual asked to supply private or confidential data concerning the individual shall be informed of:

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

When must the Tennessen warning be given?

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

- A government entity requests data;
- The data are requested from an individual;

- The data requested are private or confidential; and
- The data are about the individual from whom they are requested.

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

When is a Tennessen warning not required?

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

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

How does a government entity decide what to include in a Tennessen warning?

Preparation of a Tennessen warning should only be done by, or in close consultation with, the entity's legal advisor. Each notice must be "tailored" to the requirements of the specific entity, program, or data collection event for which it is being prepared. Within any given entity, it is likely that more than one notice will be needed.

In choosing words and phrasing for the Tennessen warning, it is important to use language that most people easily understand. The goal is to allow the data subject to make a meaningful decision to supply—or not supply—the information requested. Assuming the notice is complete and accurate, that choice can be meaningful only if the subject clearly understands the notice. Also, the subject should be given the opportunity to ask questions about the Tennessen warning and receive a clear explanation.

To protect the government entity against potential future claims, the Tennessen warning should be given in writing or in another recorded format, although the law does not specifically require it. In this regard, the individual should sign an acknowledgment that s/he has received the notice and a copy of a written notice should be given to the data subject and the original kept by the government entity with the relevant data. When information is collected over the phone, the notice should be provided orally. The entity should record such details as whether the notice was given, the date given, and the identity of the person giving the notice. If the notice is given orally, the government entity may also want to give the notice in writing as soon as practicable.

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

Private or confidential data collected before August 1, 1975 (the effective date of the Tennessen warning requirement), may be stored for the reasons the data were collected. These data also may be stored for reasons of public health, safety, or welfare, if the entity obtains the approval of the Commissioner of Administration.

Releasing Data

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

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

In order to properly respond to requests for government data, each government entity must identify the types of data it maintains and determine how each type of data is classified.

Who can make a data request?

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

What kinds of data may a person request?

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

The person may request to either inspect (or view) the data or have the government reproduce and provide a copy of that data. Generally, a governmental entity may not charge a fee for merely inspecting data, but a requesting party may be required to pay for copies or electronic transmission of data. Issues regarding whether or not a requesting person may be charged fees, and if so what activities may be subject to reimbursement and the amount of the charges, should be referred to the entity's Responsible Authority or legal counsel.

Must a government entity respond to a data request?

Once an entity has received a request, it must respond to the request appropriately and promptly. What is considered appropriate and prompt depends upon the scope of the request, and may vary depending upon such factors as the size and complexity of the entity, the type and/or quantity of data requested, the clarity of the data request, and the number of staff available to respond to the request. All data requests should be immediately referred to the Responsible Authority or legal counsel.

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

An entity may not disseminate any private or confidential data on individuals without proper legal authority. As noted, the subject of data is entitled to see data about themselves properly classified as private but may not be entitled to data classified as confidential.

If the entity determines that the requested data are not public, it must inform the requestor. This may be done orally at the time of the request, or may be done in writing as soon as possible after the request is made. When informing the requestor, the entity must cite the specific statutory section, temporary classification, or specific provision of federal law that classifies the data as private, confidential, nonpublic or protected nonpublic. Making a general statement such as, "We can't give you the data because of the data privacy act," is not an appropriate response. The entity must cite the specific section of law that classifies the data as not public.

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

A government entity may disclose private, confidential, nonpublic, or protected nonpublic data (1) if such disclosure is specifically authorized by state, local, or federal law; or (2) pursuant to an order of a District Court Judge or Administrative Hearing Officer.

The Rights of Subjects of Government Data

The MGDPA establishes specific rights for individuals who are the subjects of government data, and establishes controls on how government entities collect, store, use, and release data about individuals. The Legislature established these rights and controls because the decisions that government entities make, when using information about those individuals, can have a great effect on their lives.

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

Individual rights to access data about herself or himself

The MGDPA gives specific rights to individuals who are the subjects of government data. One of these rights is the right of the data subject to access data about him or herself:

- The data subject has the right to ask and be told whether the entity maintains data about her/him, and whether those data are classified as public, private or confidential.
- The data subject has the right to see all public and private data about her/himself.
- Under certain circumstances, data about a minor data subject may be withheld from a parent or guardian.
- The entity may not charge a fee for letting the subject see data about her/himself.

- The subject has the right to be informed of the content and meaning of public and private data about her/himself upon request.
- The subject has the right to have copies of all public and private data about her/himself.
- The entity may charge a fee for providing a data subject with copies of public and/or private data about her/himself.

Individual has the rights to challenge the accuracy and/or completeness of public and private data about her/himself.

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

Informed Consent for the Release of Government Data for Government Entities Subject to the Minnesota Government Data Practices Act

Minn. Stat. § 13.05, sub. 4, limits the subsequent use and dissemination of private or confidential data, collected from an individual, to what was described in the Tennessen warning. If the entity wishes to use or release the data in a way not communicated in the Tennessen warning, this statutory section requires the entity to obtain the individual's in-formed consent.

The standards for obtaining an informed consent are set out at Minn. Stat. § 13.05, subd. 4(d), and Minn. R. 1205.1400. A consent form must be completed in order to disseminate private data on individuals when a) the release of the data is necessary to administer or manage a legally authorized program and b) one of the following conditions applies:

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