OPEN GOVERNMENT GUIDE

Access to Public Records
and Meetings in

MINNESOTA

REPORTERS COMMITTEE
FOR FREEDOM OF THE PRESS

Sixth Edition
2011

Open Government Guide

Open Records and Meetings Laws in

MINNESOTA

Prepared by:
Paul R. Hannah
Kelly and Hannah, P.A.
3720 IDS Center
80 S. 8thSt.
Minneapolis, Minnesota 55101
(612) 349-6171

Sixth Edition
2011

OPEN GOVERNMENT GUIDE

Access to Public Records and Meetings in

MINNESOTA

SIXTH EDITION
2011

Previously Titled
Tapping Officials' Secrets

Published by The Reporters Committee for Freedom of the Press
Lucy A. Dalglish, Executive Director

EDITORS
Gregg Leslie, Legal Defense Director
Mark Caramanica, Freedom of Information Director

ASSISTANT EDITORS
Christine Beckett, Jack Nelson Legal Fellow
Aaron Mackey
Emily Peterson

Production of the sixth edition of this compendium was possible
due to the generous financial contributions of:
The Stanton Foundation

ISBN: 1-58078-224-8

Contents

Introductory Note

The OPEN GOVERNMENT GUIDE is a comprehensive guide to open government law and practice in each of the 50 states and the District of Columbia. Fifty-one outlines detail the rights of reporters and other citizens to see information and attend meetings of state and local governments.

The OPEN GOVERNMENT GUIDE — previously published as Tapping Officials' Secrets — is the sole reference on open government laws in many states.

Written to follow a standard outline to allow easy comparisons between state laws, the compendium has enabled open government advocates in one state to use arguments successful in other states to enhance access rights at home. Press associations and lobbyists have been able to invoke other sunshine laws as they seek reforms in their own.

Volunteer attorneys, expert in open government laws in each state and in Washington, D.C., generously donated their time to prepare the initial outlines for the first incarnation of this project in 1989. In most states these same attorneys or their close associates updated and rewrote the outlines for the 1993, 1997, 2001 and 2006 editions as well this current 2011 edition.

Attorneys who are new to the compendium in this edition are also experts in open government and access issues, and we are grateful to them for their willingness to share in this ongoing project to create the first and only detailed treatise on state open government law. The rich knowledge and experience all the participating attorneys bring to this project make it a success.

While most of the initial users of this compendium were journalists, we know that lawyers and citizens have discovered it and find it to be indispensable as well.

At its core, participatory democracy decries locked files and closed doors. Good citizens study their governors, challenge the decisions they make and petition or vote for change when change is needed. But no citizen can carry out these responsibilities when government is secret.

Assurances of open government exist in the common law, in the first state laws after colonization, in territorial laws in the west and even in state constitutions. All states have passed laws requiring openness, often in direct response to the scandals spawned by government secrecy. The U.S. Congress strengthened the federal Freedom of Information Act after Watergate, and many states followed suit.

States with traditionally strong access laws include Vermont, which provides virtually unfettered access on many levels; Florida, which was one of the first states to enact a sunshine law; and Ohio, whose courts have issued several access-friendly rulings. Other jurisdictions, such as Pennsylvania and the District of Columbia, have made significant changes to their respective open government laws since the fifth edition was published designed to foster greater public access to information. Historically, Pennsylvania had a reputation as being relatively non-transparent while the District of Columbia was known to have a very restrictive open meetings law.

Some public officials in state and local governments work hard to achieve and enforce open government laws. The movement toward state freedom of information compliance officers reflects a growing activism for access to information in the states.

But such official disposition toward openness is exceptional. Hardly a day goes by when we don't hear that a state or local government is trying to restrict access to records that have traditionally been public — usually because it is feared release of the records will violate someone's "privacy" or threaten our nation's security.

It is in this climate of tension between broad democratic mandates for openness and official preference for secrecy that reporters and good citizens need to garner their resources to ensure the passage and success of open government laws.

The Reporters Committee genuinely hopes that the OPEN GOVERNMENT GUIDE will help a vigorous press and citizenry to shape and achieve demands for openness, and that it will serve as a primer for those who battle in government offices and in the courts for access to records and meetings. When challenges to secrecy are successful, the news is better and so is the government.

User's Guide

Whether you are using a guide from one state to find a specific answer to an access issue, or the complete compendium encompassing all states to survey approaches to a particular aspect of open government law around the country, knowing a few basics on how the OPEN GOVERNMENT GUIDE is set up will help you to get the most out of it.

Following the outline. Every state section is based on the same standard outline. The outline is divided into two parts: access to records and access to meetings.

Start by reviewing the table of contents for each state. It includes the first two tiers of that state's outline. Once you are familiar with the structure of the outline, finding specific information is simple. Typically, the outline begins by describing the general structure of the state law, then provides detailed topical listings explaining access policies for specific kinds of records or meetings.

Every state outline follows the standard outline, but there will be some variations. Some contributors added items within the outline, or omitted subpoints found in the complete outline which were not relevant to that state's law. Each change was made to fit the needs of a particular state's laws and practices.

In general, outline points that appear in boldface type are part of the standard outline, while additional topics will appear in italicized type.

Whether you are using one state outline or any number of outlines, we think you will find the outline form helpful in finding specific information quickly without having to read an entire statute or search through many court cases. But when you do need to consult statutes, you will find the complete text of the relevant portions at the end of each outline.

Additional copies of individual state booklets, or of the compendium covering the 50 states and the District of Columbia, can be ordered from The Reporters Committee for Freedom of the Press, 1101 Wilson Blvd., Suite 1100, Arlington, Virginia 22209, or by calling (703) 807-2100. The compendium is available in electronic format on CD.

The state outlines also are available on our World-Wide Web site, www.rcfp.org/ogg. The Internet version of the outlines allows you to search the database and compare the law in different states.

Updates: The Reporters Committee published new editions of THE OPEN GOVERNMENT GUIDE in 1989, 1993, 1997, 2001, 2006, and now in 2011. We expect future updates to follow on approximately the same schedule. If we become aware of mistakes or material omissions in this work, we will post notices on this project's page on our World-Wide Web site, at www.rcfp.org/ogg. This does not mean that the outlines will constantly be updated on the site — it simply means known errors will be corrected there.

For our many readers who are not lawyers: This book is designed to help journalists, lawyers, and citizens understand and use state open records and meetings law. Although the guides were written by lawyers, they are designed to be useful to and readable by nonlawyers as well. However, some of the elements of legal writing may be unfamiliar to lay readers. A quick overview of some of these customs should suffice to help you over any hurdles.

Lawyers are trained to give a "legal citation" for most statements of law. The name of a court case or number of a statute may therefore be tacked on to the end of a sentence. This may look like a sentence fragment, or may leave you wondering if some information about that case was omitted. Nothing was left out; inclusion of a legal citation provides a reference to the case or statute supporting the statement and provides a shorthand method of identifying that authority, should you need to locate it.

Legal citation form also indicates where the law can be found in official reporters or other legal digests. Typically, a cite to a court case will be followed by the volume and page numbers of a legal reporter. Most state cases will be found in the state reporter, a larger regional reporter, or both. A case cite reading 123 A.2d 456 means the case could be found in the Atlantic (regional) reporter, second series, volume 123, starting at page 456.

Note that the complete citation for a case is often given only once. We have tried to eliminate as many cryptic second-reference cites as possible, but you may encounter cites like "Jackson at 321." This means that the author is referring you to page 321 of a case cited earlier that includes the name Jackson. Authors may also use the words supra or infra to refer to a discussion of a case appearing earlier or later in the outline, respectively.

Except for these legal citation forms, most "legalese" has been avoided. We hope this will make this guide more accessible to everyone.

Prepared by:

Paul R. Hannah
Kelly and Hannah, P.A.
3720 IDS Center
80 S. 8thSt.
Minneapolis, Minnesota 55101
(612) 349-6171

FOREWORD

In the mid-1970s, Minnesota's legislature chose to balance, by statute, openness in government with privacy interests of citizens who provide information to the government. The philosophy followed by the legislature was supposedly simple. All government data are presumptively public. The only data that are not public are data that are specifically exempted from disclosure under a specific provision of the Minnesota Government Data Practices Act (MGDPA), or some other state or federal statute.

However, in practice the presumption of openness frequently bends to various special interests. Privacy for people dealing with the government continues to be protected. Privacy interests of government employees are protected. Data that would otherwise explain government actions become unavailable when special interests within the government petition the legislature. Now, section after section of the MGDPA restricts access to important data.

Moreover, the transfer of data to digital storage has not, as one might expect, made access easier. The MGPDA has not changed to reflect this new data medium. Nervous administrators use technical questions to slow and sometimes stop access. As time passes, access becomes more complicated and more difficult.

Finally, aggrieved parties have been slow to seek redress from the courts for access problems. Litigation is expensive, and the litigation provisions of the MGDPA do not ensure recovery of fees from a government agency. As a result, there is not a significant body of decisions construing the important provisions of the MGDPA. The Commissioner of Administration has now generated a large number of opinions dealing with the law, but the opinions are not controlling, and are fairly difficult to research by the public.

In 2010, the Minnesota Legislature established an administrative remedy in addition to seeking a Commissioner's Opinion. § 13.085. An aggrieved party may file a complaint with the Office of Administrative Hearings.

The Minnesota Open Meeting Law (OML) also presumes openness. Again, though, as particular circumstances arise, Minnesota courts have shown a reluctance to give "openness" the strength it deserves. And the legislature continues to engraft exceptions to the OML which may eventually rob it of its strength.

Time will tell.

Open Records

I. STATUTE — BASIC APPLICATION

A. Who can request records?

1. Status of requestor.

Any "person" may request access to data under the Minnesota Data Practices Act. Minn.Stat. § 13.03, subd. 3(a). There is no limitation based on the status of the requester.

2. Purpose of request.

The Act does not require that the requester state a purpose when requesting data under the Act. In fact, such a requirement would seem to fly in the face of the Act's presumption that all government data "shall be public" unless otherwise classified. § 13.03, subd. 1. The only caveat to this general principle is that when a court is required to balance a benefit conferred upon the requester or the public from access against the harm created by access, the court might consider the purpose of the request to be a factor. *See e.g.* § 13.39, subd. 2a.

3. Use of records.

The Act does not restrict in any way the use of government data by the requester. However, at least one state agency has asked requesters to certify that they did not plan to repackage government information for resale.

Moreover, if a person requests access to data "that has commercial value" and was developed with a "significant expenditure of public funds," the government may charge a fee. Minn.Stat. § 13.01, subd. 3. Subdivision 3 clearly anticipates a commercial use of such valuable information.

B. Whose records are and are not subject to the act?

Generally, the Data Practices Act applies to data "collected, created, received, maintained or disseminated by a *state agency*, *political subdivision*, or *statewide system*. . ." § 13.03, subd. 1.

"State agency" is defined as "the state, the University of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district or agency of the state." Section 13.02, subd. 17. The University of Minnesota attempted to shield the names of finalists for the position of university president, arguing that its unusual position in the Minnesota Constitution rendered decisions by the Board of Regents as beyond the Data Practices Act. The Minnesota Supreme Court rejected that argument. *Star Tribune Co. v. Minnesota Bd. of Regents*, 683 N.W.2d 274, 283 (Minn. 2004).

"Political subdivision" is defined as "any county, statutory or home rule charter city, school district, special district and any board, commission, district or authority created pursuant to law, local ordinance or charter provision." The term includes nonprofit community action agencies or nonprofit social services agencies that qualify for public funds or perform services under contract to the government. Minn. Stat. § 13.02, subd. 11.

"Statewide system" is defined as a government-wide record keeping system. Minn.Stat. § 13.02, subd. 18.

1. Executive branch.

"State agency" is defined as "the state, the University of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district or agency of the state." § 13.02, subd. 17. Since the statute specifically refers to an officer of such an agency, the public data maintained by the chief executive of the agency would also be available.

a. Records of the executives themselves.

Included in section above.

b. Records of certain but not all functions.

The MGDPA does not generally define public or private data by function. However, since government data maintained by specific agencies may be the subject of a specific provision of the MGDPA, those provisions should be consulted in any particular case.

2. Legislative bodies.

The legislature was crafty enough to draft the Act so that it did not apply to the legislature. However, in 1993, as a result of a controversy over personal use of long distance telephone cards, the legislature passed legislation rendering certain records, including telephone records, public. § 10.46.

3. Courts.

Court records are subject to specific rules of access found in the Rules of Public Access to Records of the Judicial Branch. Although beyond the scope of this outline, the general principle is that "records of all courts and court administrators . . . are presumed to be open . . ." Excepted from this general rule are certain domestic abuse records, court service records, judicial work product and records otherwise made inaccessible under the various rules of practice. Furthermore, administrative records such as employee records, applicant records, security records, etc. are not available to the public.

4. Nongovernmental bodies.

a. Bodies receiving public funds or benefits.

Only governmental bodies are subject to the Data Practices Act. Those entities governed by the Data Practices Act are all "state agencies, political subdivisions and statewide systems." § 13.01, subd. 1. State agencies are defined as "the state, the University of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district or agency of the state." A "political subdivision" is "any county, statutory or home rule charter city, school district, special district and any board, commission, district or authority created pursuant to law, local ordinance or charter provision." § 13.02, subd. 11.

In addition to the above, political subdivisions also include nonprofit community action agencies or a nonprofit social service agency that performs services for a governmental entity under contract.

The MGDPA requires a government entity that contracts with a "private person" to perform any of its work to note in the contract that the government data generated by the private person are subject to the requirements of the MGDPA. § 13.05, subd. 11.

Finally, a "statewide system" is defined as "any record keeping system in which government data is collected, stored, disseminated and used by means of a system common to one or more state agencies or more than one of its political subdivisions." The Act does not define an agency subject to its provisions by the fact that it receives public funds or benefits.

b. Bodies whose members include governmental officials.

The Act does not define entities that are subject to it by their membership.

5. Multi-state or regional bodies.

If a regional body is created by the state or a political subdivision, it is governed by the Act.

6. Advisory boards and commissions, quasi-governmental entities.

If a board or commission is created by law, statute, local ordinance or charter, it is governed by the Act.

C. What records are and are not subject to the act?

1. What kind of records are covered?

The Data Practices Act does not deal with "records." It deals with "data," more specifically, "government data," which are data "collected, created, received, maintained or disseminated by any state agency, political subdivision, or statewide system regardless of its physical form, storage media or conditions of use." § 13.02, subd. 7. Mental impressions cannot be inspected or copied, and are therefore not "government data." *Navarre v. South Washington Schools*, 652 N.W.2d 9, 25 (Minn. 2002).

2. What physical form of records are covered?

All government data are subject to the act "regardless of its physical form." Thus, data in electronic formats are covered by the Act.

3. Are certain records available for inspection but not copying?

All public data are to be kept "in such an arrangement and condition as to make them easily accessible for convenient use." § 13.03, subd. 1. In addition to inspection, the public "shall be permitted to inspect and copy public government data at reasonable times and places." § 13.03, subd. 3.

D. Fee provisions or practices.

1. Levels or limitations on fees.

The Data Practices Act is very vague about specific fees and charges that may be collected. If a person requests access to data for the purpose of inspection only, the agency may not assess a charge or require the payment of a fee. If a person requests copies or "electronic transmittal" of data, agencies "*may* require the requesting person to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling, and electronically transmitting the copies of the data or the data, but may not charge for separating public from not public data." An agency may also charge a "reasonable fee" for remote access to data, if a specific statute grants that authority. § 13.03, subd. 3. Recently, agencies have begun charging for time spent in making copies of data, and such charges have been upheld. *Demers v. City of Minneapolis*, 468 N.W.2d 71 (Minn. 1991).

The Act has a specific provision dealing with requests for data that have "commercial value." § 13.03, subd. 3. If such data are developed with "a significant expenditure of public funds," the agency may charge a fee, as long as it is "clearly demonstrated" to relate to the "actual development costs." The agency is required to supply documentation to "explain and justify" the fee.

2. Particular fee specifications or provisions.

a. Search.

No fee may be charged for searching for data the requester wishes to inspect. One who requests a *copy* of the data may be asked to pay the actual costs of the search. § 13.03, subd. 3.

b. Duplication.

Duplication fees may be charged by the agency. § 13.03, subd. 3.

c. Other.

If a requester asks for a copy of electronic data in electronic form, the agency may require the requester "to pay the actual cost of providing the copy." § 13.03, subd. 3(e).

3. Provisions for fee waivers.

The Data Practices Act does not provide for fee waivers.

4. Requirements or prohibitions regarding advance payment.

The Data Practices Act does not require advance payment of fees. As a matter of practice, some agencies have asked for a commitment to pay the costs of searching and copying before beginning the work.

5. Have agencies imposed prohibitive fees to discourage requesters?

Although the practice is not widespread, persons seeking access to complete computer databases have been quoted "per record" charges which, when multiplied by the number of records in the database, resulted in prohibitive quotations. In many cases, these fees are negotiated down. As with all fees, only the "actual costs" can be assessed.

E. Who enforces the act?

A party aggrieved by a decision not to allow access may ask the Commissioner of Administration to issue an opinion with respect to the nature of the data sought. Minn.Stat.§ 13.072, subd. 1. The opinions are not binding on a public agency, but must be given deference by a court in a proceeding regarding the data. Minn.Stat.§ 13.072, subd. 2. An aggrieved party may also seek a hearing with the Office of Administrative Hearings.

1. Attorney General's role.

The Attorney General's office has no substantive role, other than her duty to issue opinions.

2. Availability of an ombudsman.

None.

3. Commission or agency enforcement.

Not specified in statute.

F. Are there sanctions for noncompliance?

See below.

II. EXEMPTIONS AND OTHER LEGAL LIMITATIONS

A. Exemptions in the open records statute.

1. Character of exemptions.

The Data Practices Act states that all data are accessible "unless classified by statute, or temporary classification pursuant to § 13.06, or federal law, as nonpublic or protected nonpublic, or with respect to data on individuals, as private or confidential." § 13.03, subd. 1.

Thus, there are no general exemptions from the Act. There are a large number of categories of data rendered non-public by specific provisions of the Act itself.

a. General or specific?

See above.

b. Mandatory or discretionary?

See above.

c. Patterned after federal Freedom of Information Act?

No.

2. Discussion of each exemption.

While the legislature attempted to draft the Data Practices Act a broadly as possible, the Act makes it clear that other provisions of other laws do not lose their force because of the existence of the Act. The Act does not create any priority. § 13.03, subd. 1.

In addition, the Act specifically refers to other rules in order to insure that no confusion arises. For example, § 13.30 makes it clear that the Act does not alter the rights and obligations of attorneys acting for the state relating to information the attorney must disclose or may protect.

A generalized exemption does exist in § 13.06. When the Data Practices Act was first drafted, an effort was made to anticipate the probability that information that should be private was overlooked. A procedure was formulated by which an agency applies to the Minnesota Department of Administration for a "temporary classification" of data as private or non-public until a proposed statute can be acted on by the legislature. The Commissioner is given 45 days in which to decide on the application. During that time, the data are deemed private. If the application is granted, the information is private until acted upon by the legislature, or until two complete legislative sessions are held without action.

B. Other statutory exclusions.

Not specified.

C. Court-derived exclusions, common law prohibitions, recognized privileges against disclosure.

See above.

D. Are segregable portions of records containing exempt material available?

Under the Act, the government is required to keep records containing government data in such a way so as to make the data easily accessible for convenient use. If the records contain public and private data, the agency "may not charge for separating public from not public data." § 13.03, subd. 3. If the public and private data cannot be segregated, the data remain private. *Northwest Publications Inc. v. City of Bloomington*, 499 N.W.2d 509, 511 (Minn.Ct.App. 1993).

E. Homeland Security Measures.

There are no specific references to homeland security in the Data Practices Act. There is an exemption for "security information" in a broad context. § 13.37, subd. 1(a). However, since the Data Practices Act specifically acknowledges the primacy of federal law, there have been instances where otherwise public data are now protected by new federal regulations.

III. STATE LAW ON ELECTRONIC RECORDS

A. Can the requester choose a format for receiving records?

The Data Practices Act does not apply to "records" but to "data." The Act makes it clear that the format of the data is not critical to its accessibility. "Photographic, photostatic, microphotographic, and microfilmed records shall be considered as accessible for convenient use regardless of the size of such records." § 13.03, subd. 1.

In addition, if an agency maintains public data "in a computer storage medium," a requester may specify a copy of the data in that medium, if the government entity "can reasonably make the copy or have a copy made." § 13.03, subd. 3(e).

B. Can the requester obtain a customized search of computer databases to fit particular needs?

There is no prohibition against requesting data that requires a customized search. However, if the requester seeks a copy of the data, the requester may be charged for the costs of "searching for and retrieving" that data. In addition, if the data has commercial value and "is a substantial and discrete portion of or an entire formula, pattern, compilation, program, device, method, technique, process, database, or system," the agency may charge a reasonable fee for the informa-

tion. Such a fee must "be clearly demonstrated by the agency to relate to the actual development costs of the information." § 13.03, subd. 3.

C. Does the existence of information in electronic format affect its openness?

Since government data are public, regardless of their format, the storage of such information in electronic format should not affect its openness. However, agencies in Minnesota are beginning to see the problems inherent in turning over large databases to requesters. Since many programs were not designed with the Act in mind, or with complete access in mind, responses to these types of requests can complicated. If, for example, a database contains both public and non-public data, an agency cannot charge for separating the data. § 13.03, subd. 3(c). However, separating such data stored in electronic format may involve complicated programming which might slow access.

D. How is e-mail treated?

The Act does not exempt e-mail from disclosure.

1. Does e-mail constitute a record?

Assuming that data in an email, and the email itself are "government data," those public data are available to the public.

2. Public matter on government e-mail or government hardware

Public matter on a public employee's computer are available to the public.

3. Private matter on government e-mail or government hardware

If a public body allows certain private data on public computers, such data are not government data, as long as they fall within the entity's policy. Advisory Opinion No. 01-075.

4. Public matter on private e-mail

See above.

5. Private matter on private e-mail

See above.

E. How are text messages and instant messages treated?

The format of the data is irrelevant if these messages contain government data, those data are available to the public.

1. Do text messages and/or instant messages constitute a record?

See above.

2. Public matter message on government hardware.

See above.

3. Private matter message on government hardware.

See above.

4. Public matter message on private hardware.

There is no specific provision dealing with public access to government data on private hardware. I assume such government data would be available to the public.

5. Private matter message on private hardware.

Such message would not be available.

F. How are social media postings and messages treated?

See above.

G. How are online discussion board posts treated?

See above.

H. Computer software

Any agency can enforce a copyright for computer software created by the agency. If the agency acquires a patent to such software, the data are treated as trade secret information pursuant to § 13.37.

1. Is software public?

See above.

2. Is software and/or file metadata public?

Metadata are not dealt with in the Act.

I. How are fees for electronic records assessed?

If government data are electronically maintained, the agency may charge for the actual costs of searching for and retrieving the data, plus the actual cost of making the copies. Minn. Stat. § 13.03, subd. 3.

J. Money-making schemes.

13.03, subd. 3(d) only allows an agency to recover its actual development costs of information with commercial value.

1. Revenues.

See above.

2. Geographic Information Systems.

Not specified.

K. On-line dissemination.

Electronic transmission of data allows the agency to recover its cost of searching for and retrieving the data, and for copy and transmitting the data. § 13.03, subd. 3(c).

IV. RECORD CATEGORIES — OPEN OR CLOSED

A. Autopsy reports.

Section 13.83 deals with "medical examiner data." Subdivision 2 describes particular data that are public; the data described are probably all a part of the usual autopsy report, although not identified as such. They include identifying information, "cause of death; causes of cause of death; whether an autopsy was performed, and if so whether it was conclusive; date and place of injury, if applicable, including work place; how injury occurred; whether death was caused by accident, suicide, homicide, or was of undetermined cause; . . ." Other data, including data that are part of the medical examiner's investigation, are private or confidential. § 13.83, subd. 4.

Section 13.83 contains one unusual provision. Subdivision 7 allows "any person" to petition the district court to authorize disclosure of private or confidential data. The court may order disclosure if it "would be in the public interest." This subdivision has been used successfully by the press.

B. Administrative enforcement records (e.g., worker safety and health inspections, or accident investigations)

Administrative enforcement data are government data and are therefore subject to the provisions of the Act.

1. Rules for active investigations.

See above.

2. Rules for closed investigations.

See above.

C. Bank records.

The Act does not refer to these records, since they are not "government data." A separate statute relates to requests by the government for data in the control of financial institutions, and does not establish any public right of access.

D. Budgets.

Notes and drafts of reports of the Department of Management and Budget are confidential until the final report has been published or is no longer being actively pursued. § 13.64, subd. 1.

E. Business records, financial data, trade secrets.

There are few specific exemptions under the Act for private sector business information held by the government.

1. Trade secret, sealed bids and security information are not public. § 13.37. However, old or limited summary financial information, such as balance sheets, hold so little information that might have value to a competitor that they may not qualify for trade secret status. *Prairie Island Indian Community v. Department of Public Safety*, 658 N.W.2d 876, 887 (Minn.Ct.App. 2003).

2. All data provided to the commissioner of public welfare by applicants for licenses under the home day care or foster care programs are public, except for personal or personal financial data. § 13.46.

3. Financial data provided to cities in the administration of economic development assistance programs are non-public until an application for assistance has been approved. § 13.62. There are other specific sections in which financial data provided with applications are non-public. (*See e.g.* Agricultural Loan and Grant Programs. § 13.643).

F. Contracts, proposals and bids.

1. Sealed bids are private data prior to the opening of bids. § 13.37, subd. 2, as are estimates for highway construction projects. § 13.72, subd. 1.

2. If the federal government requires, a state agency under contract of the federal government must keep government data private. § 13.35.

G. Collective bargaining records.

Information collected to prepare management's position and the position itself are private, if not presented during the collective bargaining process. § 13.37 subd. 2.

H. Coroners reports.

Section 13.83 deals with "medical examiner data." Subdivision 2 describes particular data that are public; the data described are probably all a part of the usual autopsy report, although not identified as such. They include identifying information, "cause of death; causes of cause of death; whether an autopsy was performed, and if so whether it was conclusive; date and place of injury, if applicable, including work place; how injury occurred; whether death was caused by accident, suicide, homicide, or was of undetermined cause; . . ." Other data, including data that are part of the medical examiner's investigation, are private or confidential. § 13.83, subd. 4.

Section 13.83 contains one unusual provision. Subdivision 7 allows "any person" to petition the district court to authorize disclosure of private or confidential data. The court may order disclosure if it "would be in the public interest." This subdivision has been used successfully by the press.

I. Economic development records.

Economic development data are now classified by a variety of statutes unrelated to the Act. For a list of statutes, see § 13.598.

J. Election records.

Sealed absentee ballots are private until opened by an election judge. § 13.37, subd. 2.

1. Voter registration records.

A public information list of voter registration records may be made available to the public. § 201.091.

2. Voting results.

Not a part of the Act.

K. Gun permits.

All data pertaining to the purchase or transfer of firearms and applications for permits to carry firearms which are collected by state agencies, political subdivisions or statewide systems are classified as private. M.S.A. 1387(c)2.

L. Hospital reports.

Public health care facilities may provide "directory information," that is, name of a patient, date admitted, and general condition. Directory information is only public during the time a person is a patient in a hospital. After that person is released, the directory information is private data on individuals. If the patient requests otherwise, the data is private. § 13.384

Directory information concerning an emergency patient who cannot communicate may be withheld until a reasonable effort is made to notify the next of kin. § 13.384, subd. 2(c).

M. Personnel records.

"Personnel data" are defined as data "collected because" a person is or was employed by or applied for a position with an agency. The definition includes those who perform voluntary services or act as an independent contractor or a member of an advisory board or commission. § 13.43, subd. 1.

Section 13.43, subd. 2, identifies the public information about current and former public employees and excludes all other information from access. The public information about current and former public employees, volunteers and independent contractors includes: name; gross salary; salary range; contract fees; annual gross pension; fringe benefits; other remuneration; job title; job description; education and training background; previous work experience; and date of first and last employment. § 13.43, subd. 2.

1. Salary.

See above.

2. Disciplinary records.

The existence and status of any complaints or charges are public. The final disposition of a disciplinary action along with reasons for the action and documenting data. § 13.43, subd. 2(4) and (5).

3. Applications.

Application data as defined in the statute are public., § 13.43, subd. 3.

4. Personally identifying information.

See above.

5. Expense reports.

Expense reports are not separately dealt with in the Act.

N. Police records.

Access to public records is governed by the Section entitled "comprehensive law enforcement data." § 13.82. Section 13.82 attempts to categorize specific actions and information that involve law enforce-

ment functions and that would, in most cases, form the nucleus of official actions. For example, subdivision 2 of the section identifies public "arrest data." Subdivision 3 requires that "request for service data," or data documenting service requests by the public, be accessible. Subdivision 4 allows access to "response or incident data," which document action taken by the law enforcement agency.

1. Accident reports.

Accident reports are confidential, except in the case of those involved. § 169.09, subd. 13(a)(1).

2. Police blotter.

Not separately dealt with in the Act. See "arrest data" in § 13.82, subd. 2.

3. 911 tapes.

Written transcription of 911 calls are public, with some caveats. Audio recordings may be used for certain public safety purposes. § 13.82, subd. 4.

4. Investigatory records.

Except for arrest and other data which are always public, while investigation is active.

Inactive investigative data are public unless their release would jeopardize another investigation or reveal the identity of a protected individual.

a. Rules for active investigations.

See above.

b. Rules for closed investigations.

See above.

5. Arrest records.

See above.

6. Compilations of criminal histories.

Criminal history data maintained by law enforcement agencies are private. The Bureau of Criminal Apprehension maintains public criminal histories. § 13.87.

7. Victims.

Data identifying victims may be withheld if the victim requests not to be identified unless the agency determines personal safety or property would not be threatened. § 13.82, subd. 17.

8. Confessions.

Not dealt with in the Act.

9. Confidential informants.

Data identifying an informant can be withheld if the agency determines that disclosure would threaten the informant's safety. § 13.82, subd. 17.

10. Police techniques.

Such data are non-public. § 13.82, subd. 25.

11. Mug shots.

While access may be delayed to assist in an investigation, booking photographs are public data. § 13.82, subd. 2(b).

12. Sex offender records.

Not dealt with in the Act. See § 241.67.

13. Emergency medical services records.

Not delath with in the Act.

O. Prison, parole and probation reports.

If these data disclose personal, medical or financial information, endanger an individual's life, endanger an investigation, identify an informant or endanger the security of an institution, the data are private, until presented to a court. § 13.85.

Most reports and/or recommendations of court services personnel, including probation and parole reports, are generally not public. § 13.84.

P. Public utility records.

Utilities and public services data are private to the extent they identify individual or prospective customers, or if they identify tenants who complain of energy efficiency problems in rental housing, or telephone company or public utility employees or customers who provide information about the possible violation of federal or state law. § § 13.679; 13.68; 13.685.

Q. Real estate appraisals, negotiations.

1. Appraisals.

Appraisal data are generally non public. § 13.44.

2. Negotiations.

Real estate negotiations are not public, but may become so when the parties enter into a purchase agreement. § 13.44.

3. Transactions.

See above.

4. Deeds, liens, foreclosures, title history.

These data are public, if filed with the relevant county office.

5. Zoning records.

Not dealt with in the Act.

R. School and university records.

1. Athletic records.

Not dealt with in the Act.

2. Trustee records.

Not dealt with in the Act.

3. Student records.

Generally, unless parties consent to "directory information," these data are private. § 13.32.

S. Vital statistics.

Generally, information contained in vital records are public. § 144.225.

1. Birth certificates.

See above.

2. Marriage & divorce.

See above.

3. Death certificates.

See above.

4. Infectious disease and health epidemics.

Not dealt with in the Act.

V. PROCEDURE FOR OBTAINING RECORDS

A. How to start.

1. Who receives a request?

The Data Practices Act requires that each agency designate an individual as the "responsible authority" in charge of requests for data. The responsible authority may identify one or more designees. § 13.02, subd. 16; § 13.03, subd. 2. As a practical matter, most requests will be dealt with by the employee whose function includes dealing with the public.

2. Does the law cover oral requests?

There is no requirement that requests for access to data be in writing.

a. Arrangements to inspect & copy.

A person shall be permitted to inspect and copy public data at reasonable times and places.

§ 13.03, subd. 3.

b. If an oral request is denied:

The responsible authority "shall inform the requesting person of the determination either orally at the time of the request, or in writing as soon after that time as possible, and shall cite the specific statutory section, temporary classification, or specific provision of federal law on which the determination is based. Upon the request of any person denied access to data, the responsible authority or designee shall certify in writing that the request has been denied and cite the specific statutory section, temporary classification, or specific provision of federal law upon which the denial was based." § 13.03, subd. 3(f).

(1). How does the requester memorialize the refusal?

A refusal shall be made either orally at the time of the request or in writing as soon as possible thereafter. A refusal shall be reduced to writing upon request. § 13.03(f).

(2). Do subsequent steps need to be in writing?

There is no provision in the Data Practices Act for an appeal within an agency after a refusal to provide information. Therefore, as a practical matter, any comments directed to any agency about such a refusal should probably be in writing.

3. Contents of a written request.

There is no format required for a written request under the Data Practices Act. A requester may even ask the responsible authority to describe the data available. If the request is for simple access to government data, there will be no fee issue. In almost all cases, the issue of a fee for compiling, gathering and copying information will be brought up by the agency subsequent to the request.

a. Description of the records.

A request should identify the data sought as specifically as possible, but there is no requirement to do so.

b. Need to address fee issues.

See above.

c. Plea for quick response.

Requests are to be complied with within an "appropriate and prompt manner." § 13.03, subd. 2(a).

d. Can the request be for future records?

There is no provision in the Act for such a request.

B. How long to wait.

It is up to the agency to arrange government data so as to "make them easily accessible for convenient use." § 13.03, subd. 1. Requests for government data must be complied with in an "appropriate and prompt manner." § 13.03, subd. 2(a). If a request for access is denied, the agency is required to cite the specific classification upon which reliance is based as "soon after that time [of the request] as possible." § 13.03, subd. 3(f).

Parties seeking access to government data are, as a practical matter, subject to the whims of the agency. Informal requests and pleas may, or may not, have any significance.

1. Statutory, regulatory or court-set time limits for agency response.

None.

2. Informal telephone inquiry as to status.

There is no such provision in the Act.

3. Is delay recognized as a denial for appeal purposes?

No.

4. Any other recourse to encourage a response.

No.

C. Administrative appeal.

Either the state agency or person requesting data may request an opinion from the Commissioner of Administration as to the public nature of the data sought. § 13.072. In addition, a person aggrieved by an alleged violation of the Act may file a complaint with the Office of Administrative Hearings. §13.085.

1. Time limit.

There is no time limit for such a Commissioner's Opinion. An administrative complaint must be filed within two years of the challenged action. § 13.085, subd. 2(b).

2. To whom is an appeal directed?

The request for opinion, normally in writing, is directed to the Commissioner of Administration. An administrative complaint is filed with the Office of Administrative Hearings.

a. Individual agencies.

None.

b. A state commission or ombudsman.

See above.

c. State attorney general.

None.

3. Fee issues.

Issues relating to a determination by an agency as to the fee to be charged for various actions taken as a result of a request for information is a proper matter for a Commissioner's opinion. Given a $1,000 fee to file an administrative complaint, §13.085, subd. 2(c), it is unlikely to be used for that purpose.

4. Contents of appeal letter.

The request for a Commissioner's opinion should contain a description of the data sought, a short chronology of the events leading up to the denial of access by the agency and the reasons given by the agency for denial. The request for an opinion should also summarize the ar-

guments refuting the agency's reasons for denial. It is wise to include any documents evidencing the positions of the parties.

An administrative complaint should detail the factual basis for the claim that a violation of law has occurred.

a. Description of records or portions of records denied.

See above.

b. Refuting the reasons for denial.

See above.

5. Waiting for a response.

If the Commissioner decides not to issue an opinion, he will provide a notice of that decision within 5 days of the receipt of the request. If the Commissioner is to issue an opinion, such an issuance is to occur within 20 days of receipt of the request. The commissioner may "for good cause" extend this deadline for one additional 30-day period. § 13.072, subd. 1(a).

Once an administrative complaint has been filed, the respondent must file a response within fifteen business days. Thereafter, an administrative law judge will discuss the claim, or set it for hearing.

6. Subsequent remedies.

Unfortunately, opinions issued by the Commissioner are not binding on the agency, but "must be given deference by a court in a proceeding involving the data." § 13.073, subd. 2. Furthermore, the procedure set forth under § 13.073 is not a condition precedent to bringing a legal action on the same issue.

A party aggrieved by a decision of the ALR may seek certiorari to the Court of Appeals.

D. Court action.

The Data Practices Act provides a cause of action for two separate sets of claimants. First, any person who suffers damage as a result of a violation of the Act may bring an action seeking recovery of those damages. § 13.08, subd. 1.

In addition to an action for damages any "aggrieved person" may bring an action to compel compliance with the provisions of the Act. § 13.08, subd. 4.

1. Who may sue?

Any person damaged may sue. The responsible authority may be sued in addition to the particular agency. § 13.08, subd. 1.

2. Priority.

In an action seeking compliance with the Act, the statute states that "the matter shall be heard as soon as possible." There is no other provision granting expedited status. § 13.08, subd. 4.

3. Pro se.

Pro se requests for Commissioner's opinions are not unusual. *Pro se* lawsuits have all the usual problems. *Pro se* administrative complaints may be problematic.

4. Issues the court will address:

The court is able to compel compliance with the provisions of the chapter. Such compliance would include access to data, the setting aside of fees, requiring a prompt action by the agency, etc. The court may impose a civil penalty and may award costs and disbursements, including attorney fees. § 13.08, subd. 4.

a. Denial.

See above.

b. Fees for records.

See above.

c. Delays.

See above.

d. Patterns for future access (declaratory judgment).

Not dealt with in the Act.

5. Pleading format.

Sec. 13.08 does not require pleading in any specific format. The assumption is that such a suit will follow the Rules of Civil Procedure.

6. Time limit for filing suit.

There is no stated statute of limitations within the Act.

7. What court.

Suit may be commenced in 1) the county where the person seeking relief resides, 2) the county where the political subdivision exists, 3) in the case of the state, any county. § 13.08, subd. 3.

8. Judicial remedies available.

Persons who suffered damage as a result of a violation of the provision of this chapter, usually parties about whom data has been wrongfully publicized, may seek damages sustained in addition to costs and reasonable attorneys' fees. If a violation is willful on the part of the agency, exemplary damages of from $100 to $10,000 are also available. § 13.08, subd. 1.

The statute also gives the court the power to enjoin an agency that had violated or proposes to violate the chapter. § 13.08, subd. 2.

In addition to an order compelling compliance, a party seeking data may recover costs and disbursements, including reasonable attorneys' fees. If the court decides that an action seeking access was frivolous, it may award reasonable costs and attorneys' fees to the agency. § 13.08, subd. 4.

9. Litigation expenses.

Parties seeking access to data *may* recover costs and attorneys' fees. § 13.08, subd. 4. Persons about whom data were wrongfully revealed may also recover costs and attorneys' fees. § 13.08, subd. 1.

a. Attorney fees.

See above.

b. Court and litigation costs.

See above.

10. Fines.

If an agency willfully discloses private information, the court may impose exemplary damages of not less than $100 and not more than $10,000 for each violation. If a court orders an agency to grant access, it may impose a civil penalty of up to $300. No such provision exists for the willful failure to provide information. § 13.08, subd. 1.

11. Other penalties.

A willful violation of the chapter may be a misdemeanor, and constitutes just cause of suspension without pay or dismissal of the public employee. § 13.09.

12. Settlement, pros and cons.

As a practical matter, given the length of time even a Commissioner's opinion can take, most media resolve disputes concerning access through negotiation. Since very few reported decisions construe the

Act, there is little precedent that compels a favorable decision.

E. Appealing initial court decisions.

There are no specific provisions dealing with the appeal of an interpretation of the Data Practices Act. If extraordinary remedies are felt to be necessary, the Minnesota Court of Appeals has specific rules that may be utilized. Rule 120, *et seq*., Minn.R.Civ.App.P. Otherwise, the normal appellate rules would apply.

1. Appeal routes.

Filing a Notice of Appeal. Rule 103.01, Minn.R.Civ.App.P.

2. Time limits for filing appeals.

An appeal from an order must be taken within 30 days after service of notice of filing. An appeal from a judgment must be taken within 60 days of entry of judgment. Rule 104.01, Minn.R.Civ.App.P.

3. Contact of interested amici.

The Reporters Committee for Freedom of the Press often files *amicus* briefs in cases involving significant media law issues before a state's highest court. In Minnesota, the Minnesota Newspaper Association also serves in an *amicus* capacity.

F. Addressing government suits against disclosure.

There is no apparent case law on this topic.

Open Meetings

I. STATUTE — BASIC APPLICATION.

A. Who may attend?

Minnesota's Open Meeting Law makes it clear that all meetings required by statute to be open are open "to the public." Minn.Stat. § 13D.01, subd. 1.

B. What governments are subject to the law?

1. State.

"Any state agency, board, commission, or department when required or permitted by law to transact public business in a meeting" shall do so in an open meeting. § 13D.01, subd. 1(a). The Minnesota Supreme Court has explicitly held that the University of Minnesota Board of Regents are subject to the provisions of the law. *Star Tribune Co. v. University of Minnesota Bd. of Regents*, 683 N.W.2d 274, 281 (Minn. 2004).

2. County.

The Open Meeting Law also applies to "the governing body of any school district however organized, unorganized territory, county, city, town, or other public body." § 13D.01, subd. 1(b).

3. Local or municipal.

The Open Meeting Law also applies to "the governing body of any school district however organized, unorganized territory, county, city, town, or other public body." § 13D.01, subd. 1(b).

C. What bodies are covered by the law?

1. Executive branch agencies.

Provided that an executive branch agency, board, commission, or department is "required or permitted by law to transact public business in a meeting," such a meeting shall abide by the provisions of the Open Meeting Law. § 13D.01, subd. 1(a).

a. What officials are covered?

The only officials involved are those who transact public business or a meeting. § 13D.01, subd. 1(a).

b. Are certain executive functions covered?

The only functions involved are those that must be taken at a public meeting. § 13D.01, subd. 1(a).

c. Are only certain agencies subject to the act?

The only entities subject to the Act are those that transact business in a public meeting. § 13D.01, subd. 1(a).

2. Legislative bodies.

The state legislature does not fall within the provisions of the Open Meeting Law. Legislative bodies of any political subdivision are subject to the provision of the Open Meeting Law. § 13D.01, subd. 1(b).

In 1990 the legislature passed a law, separate from the Open Meeting Law, requiring that all legislative meetings be open to the public. The law applies to House and Senate floor sessions, and to meetings of committees, subcommittees, conference committees and legislative commissions. For purposes of this law, a meeting occurs when a quorum is present and action is taken regarding a matter within the jurisdiction of the group. Each house of the legislature must adopt rules to implement these requirements. Remedies provided under these rules are the exclusive means of enforcing this law (Minn.Stat. § 3.055).

3. Courts.

State courts are not subject to the Open Meeting Law.

4. Nongovernmental bodies receiving public funds or benefits.

Boards of publicly owned hospitals are covered by the law. *Itasca County Board of Commissioners v. Olson*, 372 N.W.2d 804 (Minn.App. 1985). The Court of Appeals also pointed out that the county board had delegated management responsibility to the hospital board and that the county commissioners were also members of the hospital board, although the court did not differentiate between these factors.

But see the *Minnesota Daily v. University of Minnesota*, 432 N.W.2d 189 (Minn.App. 1988) in which the Court of Appeals found that the Open Meeting Law was not applicable to meetings of a committee that narrowed a list of candidates for the position of university president.

The Open Meeting Law does not refer to nonprofit corporations, even those created by the legislature. However, the law creating certain nonprofit corporations (e.g. Minnesota Technology Inc.) may specify that these groups are subject to the Open Meeting Law.

In 1986, an Attorney General's Opinion stated that the Open Meeting Law does not apply to nonprofit corporations, even if they are funded primarily with public money, are appointed by public officials, and perform services exclusively for governmental units. Op.Atty.Gen. 92a-30, January 29, 1986.

5. Nongovernmental groups whose members include governmental officials.

See Itaska County Board, supra. Generally, such groups would not be governed by the Open Meeting Law.

6. Multi-state or regional bodies.

Since a regional body is not a state agency, the Open Meeting Law would not apply to it. § 13D.01.

7. Advisory boards and commissions, quasi-governmental entities.

Assuming that the board and/or commission was established by statute and required or permitted by law to transact public business in a meeting, such meeting would be subject to the provisions of the Open Meeting Law.

8. Other bodies to which governmental or public functions are delegated.

If a public function is delegated to a committee, subcommittee, board, department or commission of a state agency, board, commission or department required or permitted to transact public business in a meeting, or the governing body of a political subdivision, then those meetings would be open to the public. If the body only performs some preliminary screening function on behalf of the public body, its meetings would probably not be subject to the provisions of the open meeting law. In *Minnesota Daily v. University of Minnesota*, 432 N.W. 2d 189 (Minn.App. 1988) an advisory committee appointed by the University Board of Regents to conduct the preliminary steps of a presidential search was held not to be a committee of the Board of Regents. Therefore, the meetings were not subject to the Open Meeting Law. The court based this ruling on the fact that no Regents were a part of the search committee, and the committee had no authority to make a final decision.

9. Appointed as well as elected bodies.

The Open Meeting Law does not limit itself to meetings of bodies of elected officials.

D. What constitutes a meeting subject to the law.

1. Number that must be present.

Meetings subject to the open meeting law "are those gatherings *of a quorum* or more members of a governing body, or a quorum of a committee, subcommittee, board, department, or commission thereof . . ." *Moberg v. Independent School Dist. No. 281*, 336 N.W.2d 510, 518 (Minn. 1983). By implication, the meeting must involve a quorum in order to be subject to the law. See also, *Columbus Concerned Citizens, Inc. v. Minn. Racing Comm'n.*, 2006 WL 1529494 (Minn. App. 2006).

In *Mankato Free Press Co. v. City of North Mankato*, 563 N.W.2d 29 (Minn.App. 1997) members of the North Mankato city council met individually, in serial fashion, with candidates for a city administrator's position. The Court of Appeals found that, while serial meetings may have the *effect* of avoiding public meetings, a fact question existed as to whether they were *designed* to do so. If that was the design, such meeting would violate the Open Meeting Law.

In another case, however, the Apple Valley, Minnesota, City Council decided to fill an open council seat by a vote. Before the vote, individual council members planned to meet privately with each applicant. The court ruled that it would not order that these sessions be open to the public, since individual council members cannot transact council business.

The court, in *dicta*, did state that it ruled in part because the council "assured this court that there will be a public hearing, in which all applicants will participate, that public input will be sought and encouraged before any decision is made and before any finalists are chosen, and that the contemplated procedure is not intended to permit council members to forge a majority prior to a public hearing or to conceal any improper influences which may affect the selection." *Northwest Publications Inc. v. City of Apple Valley*, Dakota Court File No. C7-91-332 (Feb. 27, 1991).

The court's admonition followed *dicta* in *Moberg*, where the Supreme Court commented:

> "serial meetings in groups of less then a quorum for the purposes of avoiding public hearings or fashioning agreement upon an issue may also be found to be a violation of the statute, depending upon the facts of the individual case." *Moberg*, supra, 336 N.W.2d at 518.

In 1993 a Washington County district judge held that the City Council of Hugo, Minnesota did not violate the Open Meeting Law when its members conducted separate interviews with a candidate for City Administrator. The public was allowed to attend these interviews. *Sell Publishing Co. v. City Counsel of the City of Hugo, et al.*, Washington County Court File No. CX-92-1447 (February 5, 1993.)

a. Must a minimum number be present to constitute a "meeting"?

See above.

b. What effect does absence of a quorum have?

See above.

2. Nature of business subject to the law.

a. "Information gathering" and "fact-finding" sessions.

Previously scheduled informational seminars about school board business, attended by the entire board, are subject to the Open Meeting Law and must be publicized and open. *St. Cloud Newspapers Inc. v. District 742 Community Schools*, 332 N.W.2d 1, 6 (Minn. 1983). In that decision, the court held that "chance or social gatherings" are not subject to the Open Meeting Law, even if a quorum is present.

There is a countervailing notion that attendance at a general training session might not be subject to the Open Meeting Law, if the agenda relates to the general performance of their duties. *See* Op.Atty. Gen. 63a-5, Feb. 5, 1995. *Duluth News-Tribune v. Krueger, et al.*, St. Louis County District Court File No. C8-93-601228 (Dec. 30, 1993).

b. Deliberations toward decisions.

Any "scheduled" gathering of members of a governing body must be open, even if action is not contemplated. This includes meetings where information is received that "may" influence later actions. *St. Cloud Newspapers Inc.*, *supra*, 332 N.W.2d at 6. The term "meetings" is to be "broadly interpreted."

3. Electronic meetings.

Meetings by telephone or other electronic means are governed by § 13D.015, passed in 2009. The statute applies to state agencies, boards, commissions, departments, or statewide public pension plans, and committees, etc. thereof. In order to proceed, all members must be able to hear each other and any discussion, members of the public must have the same access, one member must be physically present at the regular hearing place, and all must be conducted by role call. § 13D.013, subd. 2. People may also monitor the meeting by electronic means if feasible. § 13D.015, subd. 4. Notice shall be provided, along with the fact that some members may participate by electronic means. In addition to the regular method of notice, the entity must post its notice on its website within ten days of the meeting.

§ 13D.015, subd. 5. (For meeting by "interactive television," see § 13D.02.

a. Conference calls and video/Internet conferencing.

See above.

b. E-mail.

Proposed legislation to allow e-mail meetings has not been passed by the Minnesota Legislature.

c. Text messages.

See above.

d. Instant messaging.

See above.

e. Social media and online discussion boards.

See above.

E. Categories of meetings subject to the law.

1. Regular meetings.

a. Definition.

By implication, any regularly scheduled meeting, that is, one that is held at a regularly scheduled time and place, is a "regular" meeting. Although the term "regular" meeting is used in the statute, it is not otherwise defined. § 13D.04, subd. 1.

b. Notice.

The only notice required of a "regular" meeting is that a schedule of those meetings of a public body "shall be kept on file at its primary offices." § 13D.04, subd. 1. (Some public bodies are required to set dates with meetings on an annual basis. *See* § 375.07 with respect to county boards.)

The Minnesota Supreme Court has held that the statute, which does not expressly require that notice of a regular meeting be given, must be construed to require "adequate" notice to the public. *Sullivan v. Credit River Township*, 299 Minn. 170, 174, 217 N.W.2d 502, 506 (1974). It is a violation of the Open Meeting Law to conduct business before the time publicly announced for the meeting. *Merz v. Leitch*, 342 N.W.2d 141 (Minn. 1984).

If a public body decides to hold a regular meeting at a time or place different from the time or place listed on the schedule, it must give notice as if the meeting were a special meeting. § 13D.04, subd. 1.

(1). Time limit for giving notice.

No time limit is set.

(2). To whom notice is given.

The Open Meeting Law does not provide for any notice of regular meetings other than a written schedule.

(3). Where posted.

There is no specific posting requirement. Notice need only be "adequate." However, notices must be posted in an area accessible to the public.

(4). Public agenda items required.

If printed materials relating to agenda items are prepared by or at the direction of the governing body, and are distributed or available to those members, one copy of those materials shall be available in the meeting room for inspection by the public. § 13D.01, subd. 6.

(5). Other information required in notice.

None.

(6). Penalties and remedies for failure to give adequate notice.

There are no penalties for failure to give notice separate from the $300 civil penalty set forth for *any* institutional violation. § 471.705, subd. 2.

c. Minutes.

(1). Information required.

The Open Meeting Law does not specifically require that minutes be taken of events occurring at a regular meeting. All that is required by the statute is that votes taken at a meeting required to be public will be recorded in a journal kept for that purpose, which shall be open to the public during normal business hours. If the issue involves the appropriation of money, the vote of each member shall be recorded. § 13D.01, subd. 4.

(2). Are minutes public record?

Presumably, any minutes actually taken would be public government data. The vote journal called for by § 13D.01, subd. 4 is public. § 13D.01, subd. 5.

2. Special or emergency meetings.

a. Definition.

"Special" meetings are dealt with extensively in § 13D.04, subd. 2. but are not explicitly defined by the statute. An "emergency meeting" is a "special meeting called because of circumstances that, in the judgment of the public body, require immediate consideration by the public body." § 13D.04, subd. 3.

b. Notice requirements.

(1). Time limit for giving notice.

The public body must give three days written notice of the date, time, place and purpose of this special meeting. § 13D.04, subd. 2. There is no time limit for giving notice of an emergency meeting. Section 13D.04, subd. 3. does indicate that the notice required for an emergency meeting to the public must be given "as soon as reasonably practicable after notice has been given to the members."

(2). To whom notice is given.

In addition to posting the notice, the public body must mail or deliver a copy of the notice to each person who has filed a written request for notice of special meetings with the public body. Before emergency meetings, after the members of the public body have been notified by telephone or other method, the public body "shall make good faith

efforts to provide notice of the meeting to each news medium that has filed a written request for notice if the request includes the news medium's telephone number." § 13D.04, subd. 3.

(3). Where posted.

The statute requires that notice of special meetings be posted "on the principal bulletin board of the public body, or if the public body has no principal bulletin board, on the door of its usual meeting room." It must also be mailed to those persons who have filed a written request to receive such notices. § 13D.04, subd. 2.

In *Rupp v. Mayasich*, 533 N.W.2d 893, 895 (Minn. App. 1995), the "principal" bulletin board of the Department of Transportation was located in an area separate from the reception area of the office and was not always accessible. The Court of Appeals held that "a principal bulletin board must be located in a place that is reasonably accessible to the public."

Section § 13D.04, subd. 3, dealing with emergency meetings does not contemplate the formal posting of a notice.

As an alternative to mailing notices of special meetings to persons who filed written requests for notice thereof, the public body may publish the notice once, at least three days before the meeting, in the official newspaper of the public body. § 13D.04, subd. 2.

(4). Public agenda items required.

The notice of a special meeting shall include the "purpose of the meeting."

(5). Other information required in notice.

No other information is required.

(6). Penalties and remedies for failure to give adequate notice.

No separate penalties exist for inadequate notice.

c. Minutes.

There is no specific requirement for minutes of a special meeting. There is also no specific requirement of minutes of an emergency meeting, except that "if matters not directly related to the emergency are discussed or acted upon at an emergency meeting, the minutes of the meeting shall include the description of the matters." § 13D.04, subd. 3.

(1). Information required.

No specific information is required.

(2). Are minutes a public record?

Presumably, minutes are public data under the Data Practices Act.

3. Closed meetings or executive sessions.

a. Definition.

The statute does not define a closed meeting. It defines the subject matter of the meetings that are exempt from the provisions of the Open Meeting Law. Interestingly enough, executive sessions of any governing body are treated no differently than a meeting of the entire body. § 13D.01, subd. 1.

b. Notice requirements.

The Open Meeting Law states that its notice requirements apply to closed meetings. § 13D.04, subd. 5. Thus, the general notice requirements under the open meeting law for regular, special and emergency meetings would also apply to closed meetings.

In addition, if a public body decides to hold a closed meeting "to consider strategy for labor negotiations, including negotiation strategies or developments or discussion and review of labor negotiation proposals" the time and place of the closed meeting shall be announced in the public meeting. § 13D.03, subd. 1(c).

(1). Time limit for giving notice.

See above.

(2). To whom notice is given.

See above.

(3). Where posted.

See above.

(4). Public agenda items required.

See above.

(5). Other information required in notice.

See above.

(6). Penalties and remedies for failure to give adequate notice.

See above.

c. Minutes.

As with open meetings, there is no requirement that minutes be kept of a closed meeting. If a public body closes a meeting to evaluate the performance of an employee, the public body must "summarize it conclusions regarding the evaluation" at its next open meeting. § 13D.05, subd. 3(a). If a meeting is closed pursuant to Section 13D.03 for labor negotiations, a written roll of the members and other persons present at the closed meeting is to be made public after the meeting. § 13D.03, subd. 1(d). In addition, proceedings of a closed meeting to discuss negotiation strategies must be tape recorded and be made available after all labor contracts are signed.

(1). Information required.

No specific information is required.

(2). Are minutes a public record?

Only the written roll of members and others attending a labor negotiation session is to be made public. After all labor contracts are signed, a tape recording of such a session is to be made available to the public. § 13D.03, subd. 2.

d. Requirement to meet in public before closing meeting.

With respect to all closed meetings, a public body must state its reasons "on the record" before closing a meeting. § 13D.01, subd. 3. This reference to "the record" presumes a public meeting.

If a public proposes to close a meeting to discuss labor negotiations, the time and place of the closed meeting must be announced at a public meeting. § 13D.03, subd. 1(c).

If the meeting to be closed is regular, special or emergency, the public body must follow the notice provisions that apply to the particular type of meeting to be closed. § 13D.04, subd. 5.

If a public body proposes to close a meeting to evaluate the performance of an individual subject to its authority, it must identify the individual at an open meeting, prior to closing the meeting. § 13D.05, subd. 3(a).

e. Requirement to state statutory authority for closing meetings before closure.

Section 13D.01, subd. 3 requires that the body state on the record the "specific grounds" that permit the meeting to be closed and to "describe the subject to be discussed." A public body must vote at a public meeting to hold a closed meeting to discuss labor negotiations. § 13D.03, subd. 1(b).

f. Tape recording requirements.

There is no general requirement to record closed meetings. However, if a meeting is called pursuant to Section 13D.03, subd. 2. to discuss labor negotiations, those proceedings shall be tape recorded and the recording preserved for two years after the contract at issue is signed. The tape is to be made available to the public "after all labor contracts are signed by the governing body for the current budget."

F. Recording/broadcast of meetings.

1. Sound recordings allowed.

The Open Meeting Law is silent on this issue. As a matter of practice, many public bodies regularly televise their meetings and make the telecasts available on local access cable channels. There has been no dispute concerning whether members of the public may individually record those television broadcasts.

2. Photographic recordings allowed.

Again, the Open Meeting Law is silent. The issue is one to be decided by each body.

G. Are there sanctions for noncompliance?

For intentional violations of the open meetings law, a court may assess each person a civil penalty of less than $300. Minn. Stat. Ann. § 13D.06, subd. 1. Courts have also held officials can be removed from office for violations of the open meetings law. See Claude v. Collins, 518 N.W.2d 836 (Minn.1994). If a person violates the open meetings law three or more times, they forfeit any right to serve the offending government body for the length of their term of office. § 13D.06, subd. 3. A court may award up to $13,000 in attorney's fees to the prevailing party. § 13D.06, subd. 4. Additionally, the open meetings law requires all closed meetings be recorded, and the recording can be made public by a court if the meeting was improperly closed. § 13D.03, subd. 2.

II. EXEMPTIONS AND OTHER LEGAL LIMITATIONS

A. Exemptions in the open meetings statute.

1. Character of exemptions.

a. General or specific.

The exemptions under the Open Meeting Law are specific.

b. Mandatory or discretionary closure.

The exemptions for meetings of the commissioner of corrections, and for a state agency, board or commission when it is exercising quasi-judicial functions involving disciplinary proceedings are mandatory. § 13D.01, subd. 2. Any portion of a meeting *must* be closed if the public body plans to discuss data identifying certain crime victims, active investigative data relating to misconduct of law enforcement personnel, or non-public educational, health, medical, welfare or mental health data. § 13D.05, subd. 2(c). A public body *shall* close a meeting for preliminary consideration of allegations or charges against a public employee. § 13D.05, subd. 2(b).

Closing meetings on other topics is discretionary.

2. Description of each exemption.

The Open Meeting Law excludes from its terms meetings of the commissioner/corrections and "any state agency, board, or commission when exercising quasi-judicial functions involving disciplinary proceedings." Therefore, those agencies performing those functions need not comply with *any* of the provisions of the law, including the notice provisions. § 13D.01, subd. 2.

These are the only meetings exempt from the statute for all purposes. The remaining categories of closed meetings are still governed by the Open Meeting Law.

The remaining exemptions permit meetings to be closed, but may require notice and otherwise be governed by the act. Those exemptions include exemptions for labor negotiations (§ 13D.03, subd. 1), preliminary consideration of allegations or charges against an individual subject to its authority (§ 13D.05, subd. 2(b)), performance evaluations (§ 13D.05, subd. 3(a)), meetings to discuss particular types of data made non-public under the Data Practices Act (§ 13D.05, subd. 2) meetings involving attorney-client privileged communications (§ 13D.05, subd. 3(b)), and meetings involving the proposed purchase or sale of real or personal property by the public body. (§ 13D.05, subd.3(c)).

B. Any other statutory requirements for closed or open meetings.

No other general requirements exist.

C. Court mandated opening, closing.

No court decisions mandate open or closed meetings separate from the Open Meeting Law.

III. MEETING CATEGORIES — OPEN OR CLOSED.

A. Adjudications by administrative bodies.

The provisions of the Open Meeting Law are not applicable to a state agency, board or commission when it exercises quasi-judicial functions involving disciplinary proceedings. § 13D.01, subd. 2.

1. Deliberations closed, but not fact-finding.

The Open Meeting Law allows preliminary consideration of disciplinary matters to be conducted in closed meetings, but requires subsequent meetings to be open. § 13D.05, subd. 2(b).

2. Only certain adjudications closed, i.e. under certain statutes.

The Open Meeting Law does not make this distinction.

B. Budget sessions.

Open.

C. Business and industry relations.

Open.

D. Federal programs.

Open.

E. Financial data of public bodies.

Open.

F. Financial data, trade secrets or proprietary data of private corporations and individuals.

Open, although in a discussion of data protected under the Data Practices Act, which might include certain private financial data, the data remains protected, and the public body may discuss such data without fear of liability. § 13D.05, subd. 1.

G. Gifts, trusts and honorary degrees.

Open.

H. Grand jury testimony by public employees.

Meetings of a grand jury do not fall within the provisions of the Open Meeting Law.

I. Licensing examinations.

Most state licensing agencies do not conduct their business in meetings. Therefore, the Open Meeting Law would not apply.

J. Litigation; pending litigation or other attorney-client privileges.

Prior to 1990, an exception for attorney-client communications was created by the Minnesota Supreme Court in *Minneapolis Star & Tribune Co. v. HRA*, 251 N.W.2d 620 (1976). Later, the Court described the privilege as a "very limited exception to the Open Meeting Law for attorney-client meetings." *St. Cloud Newspapers v. District 742 Community Schools*, 332 N.W.2d 1, 5 (Minn. 1983). The Court said that this exception is to be employed or invoked "cautiously, and seldom in situations other than in relation to threatened or pending litigation." In 1990 the statute was amended to include a statement that "meetings may be closed if the closure is expressly authorized by statute or permitted by the attorney-client privilege." § 13D.05, subd. 3(b).

There have been several reported decisions that have discussed the phrase "threatened or pending litigation." In *Northwest Publications Inc. v. City of St. Paul*, 435 N.W.2d 64 (Minn.App. 1989), *review denied*, the court held that the attorney-client privilege exception "properly applies when a governing body seeks legal advice concerning litigation strategy." Even if the privilege can be invoked, the public body must "demonstrate that the need for confidentiality outweighs the right of the public to have access to public affairs."

Thereafter, in 1993, the Court of Appeals construed the privilege to apply to "circumstances where litigation is imminent, but not actually commenced," or when the public body "needs advice above the level of general legal advice, i.e., regarding specific acts and their legal consequences." *Star Tribune v. Board of Education, Special School Dist. No. 1*, 507 N.W.2d 869 (Minn. App. 1993).

The Minnesota Supreme Court has ruled that, because the attorney-client privilege exception only applies when there is a need for strict confidentiality, the scope of the privilege is narrower for public bodies than for private clients. *Prior Lake American v. Mader*, 642 N.W.2d 729, 737 (Minn. 2002). However, the Minnesota Court of Appeals has limited the effect of the *Prior Lake American* decision by broadly defining the circumstances that would amount to "seriously considering legal action." In *Brainerd Daily Dispatch v. Deben*, 693 N.W.2d 435, 441-42 (2005) the Court of Appeals relied heavily on the affidavit of the lawyer for a public body in determining whether the proper standard had been met in closing a meeting to discuss threatened litigation. The Court of Appeals found that a factor is whether the private meeting would contribute to litigation strategy.

K. Negotiations and collective bargaining of public employees.

1. Any sessions regarding collective bargaining.

Under § 13D.03, subd. 1(b)., a public employer may hold a closed meeting "to consider strategy for labor negotiations, including negotiation strategies or developments or discussion and review of labor negotiation proposals."

2. Only those between the public employees and the public body.

The Public Employment Labor Relations Act (PELRA) provides that "negotiations, mediation sessions and hearings between public employers and public employees" are public meetings, "except when otherwise provided by the director [mediator]." § 179.69, subd. 2.

This statute has been construed to mean that a mediator may decide that a meeting is closed in her discretion, even if the meeting does not include both parties to the mediation process. *Minnesota Education Association v. Bennet*, 321 N.W.2d 395 (Minn. 1982).

L. Parole board meetings, or meetings involving parole board decisions.

Presumably open, if meetings or hearings are conducted. The statutes do not specifically require a meeting or a hearing. § 243.05.

M. Patients; discussions on individual patients.

Under § 13D.05, subd. 2(a)(3). a meeting must be closed if health data or medical data that would include patient information is to be discussed.

N. Personnel matters.

1. Interviews for public employment.

There is no specific provision of the Open Meeting Law that would allow the public body itself, or a quorum thereof, to close an interview of a perspective employee. On the other hand, interviews of such applicants have been the subject of "serial" meetings that have, to this point, passed muster.

2. Disciplinary matters, performance or ethics of public employees.

Under the 1990 amendment, a public body *may* close a meeting to "evaluate the performance of an individual who is subject to its authority." The public body must identify the person to be evaluated prior to closing the meeting. Thereafter, the public body must summarize its conclusions regarding the evaluation. The meeting may be open at the request of the individual who is the subject of the meeting. § 13D.05, subd. 3(a).

Furthermore "a public body shall close one or more meetings for preliminary consideration of allegations or charges against an individual subject to its authority." If the body concludes that discipline may be warranted, further meetings or hearings relating to those specific charges or allegations must be open. The meeting must also be open at the request of the individual who is the subject of the meeting. § 13D.05, subd. 2(b).

3. Dismissal; considering dismissal of public employees.

Depending on the reason for dismissal, such meetings should be open. § 13D.05, subd. 3(a) and 2(b).

O. Real estate negotiations.

Closed. § 13D.05, subd. 3(c).

P. Security, national and/or state, of buildings, personnel or other.

Open.

Q. Students; discussions on individual students.

Hearings on the exclusion and expulsion of public school students shall be closed. § 127.31.

IV. PROCEDURE FOR ASSERTING RIGHT OF ACCESS

A. When to challenge.

Challenges to decisions to close public meetings have occurred both before and after the scheduled meeting. While the statute does not provide for injunctive relief, several reported decisions involve such a request. The law itself does not require that a court expedite such a challenge.

1. Does the law provide expedited procedure for reviewing request to attend upcoming meetings?

No.

2. When barred from attending.

This is a ground for challenging a decision to close.

3. To set aside decision.

Courts have held that courts cannot void the decisions made at meetings improperly closed. See *Columbus Concerned Citizens, Inc. v.*

Minnesota Racing Comm'n., 2006 WL 1529494 (Minn. App. 2006).

4. For ruling on future meetings.

Courts have issued declaratory judgments with respect to future meetings.

5. Other.

No court decision has established a principle of expedited review of decisions relating to close meetings.

B. How to start.

The only forum available to challenge closure decisions is an action in state district court.

1. Where to ask for ruling.

a. Administrative forum.

(1). Agency procedure for challenge.

None exists.

(2). Commission or independent agency.

None exists.

b. State attorney general.

The Attorney General can issue opinions, but rarely does so. Such opinions may have impact in the pending dispute, and have limited precedential value.

c. Court.

An action in state district court is the only forum available to challenge closure decisions.

2. Applicable time limits.

None are stated in the statute.

3. Contents of request for ruling.

There is no standard pleading.

4. How long should you wait for a response?

Timeliness is important, but not required.

5. Are subsequent or concurrent measures (formal or informal) available?

No.

C. Court review of administrative decision.

1. Who may sue?

Any person may bring suit.

2. Will the court give priority to the pleading?

There is no provision in the law granting priority.

3. Pro se possibility, advisability.

It is certainly possible to act *pro se*, but it is not advisable.

4. What issues will the court address?

a. Open the meeting.

If a body does not hold a closed meeting before suit, the effect of an adverse judgment is to open the meeting.

b. Invalidate the decision.

Previously, the Supreme Court held that parties could seek an order rendering the decision taken at a wrongfully closed meeting invalid. *Quast v. Knutson*, 276 Minn. 340, 150 N.W.2d 199 (1968). After the legislature amended the Open Meeting Law to include civil penalties, the Supreme Court concluded that invalidation was not available. *Sullivan v. Credit River Township*, 217 N.W.2d 502 (Minn. 1974). See *Columbia Concerned Citizens*, supra.

c. Order future meetings open.

Such an order is possible.

5. Pleading format.

Standard pleadings are expected.

6. Time limit for filing suit.

The statute sets no specific limitations.

7. What court.

County in which public body is located. If a state agency, any county.

8. Judicial remedies available.

Injunctive relief may be an appropriate remedy, provided the relief does not alter the purpose of the statute, involves matters actually litigated and sets forth its order with reasonable certainty. *Channel 10 Inc. v. Independent School Dist. No. 709*, 298 MN 306, 215 N.W.2d 814 (1974). Governing bodies have sought orders declaring a proposed act as an appropriate subject of an open meeting. *Itaska County Board of Commissioners*, 372 N.W.2d 804 (Minn. App. 1985).

9. Availability of court costs and attorneys' fees.

The court may award reasonable costs, disbursements, and fees of up to $13,000 to any party in the action. § 13D.06, subd. 4(a). No attorneys fees may be awarded against a member of the public body unless the court finds there was a specific intent to violate the law. § 13D.06, subd. 4(a). The court may also award costs and fees to a defendant, but it must find the action was frivolous and without merit. § 13D.06, subd. 4(b).

10. Fines.

A person who "intentionally" violates the Open Meeting Law is subject to a civil penalty in an amount not to exceed $300 for a single occurrence, which cannot be paid by the public body. § 13D.06, subd. 1.

11. Other penalties.

If a person is found by the court to have "intentionally violated" the Open Meeting Law in three or more actions, "such person shall forfeit any further right to serve on such governing body or in any other capacity with such public body for a period of time equal to the term of office such person was then serving." § 13D.06, subd. 3.

D. Appealing initial court decisions.

Normal appellate procedures apply to actions reviewing trial court decisions relating to the Open Meeting Law. If extraordinary remedies are felt to be necessary, the Minnesota Court of Appeals has specific rules which may be utilized. *See* Rule 120, *et seq.*, Minn.R.Civ. App.P.

1. Appeal routes.

Filing a Notice of Appeal. Rule 103.01, Minn.R.Civ.App.P.

2. Time limits for filing appeals.

An appeal from an order must be taken within 30 days after service of notice of filing. An appeal from a judgment must be taken within 60 days of entry of judgment. Rule 104.01, Minn.R.Civ.App.P.

3. Contact of interested amici.

The Reporters Committee for Freedom of the Press, the Minnesota Newspaper Association and other professional organizations often file *amicus* briefs in cases involving significant media law issues before a state's highest court.

V. ASSERTING A RIGHT TO COMMENT.

A. Is there a right to participate in public meetings?

The Open Meeting Law does not, by its terms, grant a right to comment at public meetings. Court decisions have held that one of the purposes of the statute is to "give the public an opportunity to express its views." *Claude v. Collins*, 518 N.W.2d 836, 841 (Minn. 1994). However, there are no reported decisions involving the denial of a right to participate.

B. Must a commenter give notice of intentions to comment?

There are no general rules. Rules are established by each public body.

C. Can a public body limit comment?

There are no general rules. Rules are established by each public body.

D. How can a participant assert rights to comment?

There are no general rules. Rules are established by each public body.

E. Are there sanctions for unapproved comment?

There are no general rules. Rules are established by each public body.

Statute

Open Records

Minnesota Statutes Annotated

Data Practices (Ch. 13-13C)

Chapter 13. Government Data Practices

Generally

13.01. Government data

Subdivision 1. Applicability. All government entities shall be governed by this chapter.

Subd. 2. Citation. This chapter may be cited as the "Minnesota Government Data Practices Act."

Subd. 3. Scope. This chapter regulates the collection, creation, storage, maintenance, dissemination, and access to government data in government entities. It establishes a presumption that government data are public and are accessible by the public for both inspection and copying unless there is federal law, a state statute, or a temporary classification of data that provides that certain data are not public.

Subd. 4. Headnotes. The headnotes printed in boldface type before paragraphs in this chapter are mere catchwords to indicate the content of a paragraph and are not part of the statute.

Subd. 5. Provisions coded in other chapters.

(a) The sections referenced in this chapter that are codified outside this chapter classify government data as other than public, place restrictions on access to government data, or involve data sharing.

(b) Those sections are governed by the definitions and general provisions in sections 13.01 to 13.07 and the remedies and penalties provided in sections 13.08 and 13.09, except:

(1) for records of the judiciary, as provided in section 13.90; or

(2) as specifically provided otherwise by law.

13.02. Collection, security, and dissemination of records; definitions

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

Subd. 2. Commissioner. "Commissioner" means the commissioner of the department of administration.

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

Subd. 3a. Criminal justice agencies. "Criminal justice agencies" means all state and local prosecution authorities, all state and local law enforcement agencies, the sentencing guidelines commission, the bureau of criminal apprehension, the department of corrections, and all probation officers who are not part of the judiciary.

Subd. 4. Data not on individuals. "Data not on individuals" means all government data which is not data on individuals.

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

Subd. 6. Designee. "Designee" means any person designated by a respon-

sible authority to be in charge of individual files or systems containing government data and to receive and comply with requests for government data.

Subd. 7. Government data. "Government data" means all data collected, created, received, maintained or disseminated by any government entity regardless of its physical form, storage media or conditions of use.

Subd. 7a. Government entity. "Government entity" means a state agency, statewide system, or political subdivision.

Subd. 8. Individual. "Individual" means a natural person. In the case of a minor or an individual adjudged mentally incompetent, "individual" includes a parent or guardian or an individual acting as a parent or guardian in the absence of a parent or guardian, except that the 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 that withholding the data would be in the best interest of the minor.

Subd. 8a. Not public data. "Not public data" means any government data which is classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic.

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

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

Subd. 11. Political subdivision. "Political subdivision" means any county, statutory or home rule charter city, school district, special district, any town exercising powers under chapter 368 and located in the metropolitan area, as defined in section 473.121, subdivision 2, and any board, commission, district or authority created pursuant to law, local ordinance or charter provision. It includes any nonprofit corporation which is a community action agency organized pursuant to the Economic Opportunity Act of 1964 (Public Law Number 88-452) as amended, to qualify for public funds, or any nonprofit social service agency which performs services under contract to any political subdivision, statewide system or state agency, to the extent that the nonprofit social service agency or nonprofit corporation collects, stores, disseminates, and uses data on individuals because of a contractual relationship with state agencies, political subdivisions or statewide systems.

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

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

Subd. 14. Public data not on individuals. "Public data not on individuals" means data which is accessible to the public pursuant to section 13.03.

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

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

Subd. 17. State agency. "State agency" means the state, the University of Minnesota, and any office, officer, department, division, bureau, board, commission, authority, district or agency of the state.

Subd. 18. Statewide system. "Statewide system" includes any record-keeping system in which government data is collected, stored, disseminated and used by means of a system common to one or more state agencies or more than one of its political subdivisions or any combination of state agencies and political subdivisions.

Subd. 19. Summary data. "Summary data" means statistical records and reports derived from data on individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.

13.03. Access to government data

Subdivision 1. Public data. All government data collected, created, received, maintained or disseminated by a government entity shall be public unless classified by statute, or temporary classification pursuant to section 13.06, or federal law, as nonpublic or protected nonpublic, or with respect to data on individuals, as private or confidential. The responsible authority in every government entity shall keep records containing government data in such an arrangement and condition as to make them easily accessible for convenient use. Photographic, photostatic, microphotographic, or microfilmed records shall be considered as accessible for convenient use regardless of the size of such records.

Subd. 2. Procedures.

(a) The responsible authority in every government entity shall establish procedures, consistent with this chapter, to insure that requests for government data are received and complied with in an appropriate and prompt manner.

(b) The responsible authority shall prepare public access procedures in written form and update them no later than August 1 of each year as necessary to reflect any changes in personnel or circumstances that might affect public access to government data. The responsible authority shall make copies of the written public access procedures easily available to the public by distributing free copies of the procedures to the public or by posting a copy of the procedures in a conspicuous place within the government entity that is easily accessible to the public.

(c) Full convenience and comprehensive accessibility shall be allowed to researchers including historians, genealogists and other scholars to carry out extensive research and complete copying of all records containing government data except as otherwise expressly provided by law.

A responsible authority may designate one or more designees.

Subd. 3. Request for access to data.

(a) Upon request to a responsible authority or designee, a person shall be permitted to inspect and copy public government data at reasonable times and places, and, upon request, shall be informed of the data's meaning. If a person requests access for the purpose of inspection, the responsible authority may not assess a charge or require the requesting person to pay a fee to inspect data.

(b) For purposes of this section, "inspection" includes, but is not limited to, the visual inspection of paper and similar types of government data. Inspection does not include printing copies by the government entity, unless printing a copy is the only method to provide for inspection of the data. In the case of data stored in electronic form and made available in electronic form on a remote access basis to the public by the government entity, inspection includes remote access to the data by the public and the ability to print copies of or download the data on the public's own computer equipment. Nothing in this section prohibits a government entity from charging a reasonable fee for remote access to data under a specific statutory grant of authority. A government entity may charge a fee for remote access to data where either the data or the access is enhanced at the request of the person seeking access.

(c) The responsible authority or designee shall provide copies of public data upon request. If a person requests copies or electronic transmittal of the data to the person, the responsible authority may require the requesting person to pay the actual costs of searching for and retrieving government data, including the cost of employee time, and for making, certifying, compiling, and electronically transmitting the copies of the data or the data, but may not charge for separating public from not public data. However, if 100 or fewer pages of black and white, letter or legal size paper copies are requested, actual costs shall not be used, and instead, the responsible authority may charge no more than 25 cents for each page copied. If the responsible authority or designee is not able to provide copies at the time a request is made, copies shall be supplied as soon as reasonably possible.

(d) When a request under this subdivision involves any person's receipt of copies of public government data that has commercial value and is a substantial and discrete portion of or an entire formula, pattern, compilation, program, device, method, technique, process, database, or system developed with a significant expenditure of public funds by the government entity, the responsible authority may charge a reasonable fee for the information in addition to the costs of making, certifying, and compiling the copies. Any fee charged must be clearly demonstrated by the government entity to relate to the actual development costs of the information. The responsible authority, upon the request of

any person, shall provide sufficient documentation to explain and justify the fee being charged.

(e) The responsible authority of a government entity that maintains public government data in a computer storage medium shall provide to any person making a request under this section a copy of any public data contained in that medium, in electronic form, if the government entity can reasonably make the copy or have a copy made. This does not require a government entity to provide the data in an electronic format or program that is different from the format or program in which the data are maintained by the government entity. The entity may require the requesting person to pay the actual cost of providing the copy.

(f) If the responsible authority or designee determines that the requested data is classified so as to deny the requesting person access, the responsible authority or designee shall inform the requesting person of the determination either orally at the time of the request, or in writing as soon after that time as possible, and shall cite the specific statutory section, temporary classification, or specific provision of federal law on which the determination is based. Upon the request of any person denied access to data, the responsible authority or designee shall certify in writing that the request has been denied and cite the specific statutory section, temporary classification, or specific provision of federal law upon which the denial was based.

Subd. 4. Change in classification of data; effect of dissemination among agencies.

(a) The classification of data in the possession of an entity shall change if it is required to do so to comply with either judicial or administrative rules pertaining to the conduct of legal actions or with a specific statute applicable to the data in the possession of the disseminating or receiving entity.

(b) If data on individuals is classified as both private and confidential by this chapter, or any other statute or federal law, the data is private.

(c) To the extent that government data is disseminated to a government entity by another government entity, the data disseminated shall have the same classification in the hands of the entity receiving it as it had in the hands of the entity providing it.

(d) If a government entity disseminates data to another government entity, a classification provided for by law in the hands of the entity receiving the data does not affect the classification of the data in the hands of the entity that disseminates the data.

Subd. 5. Copyright or patent of government data. A government entity may enforce a copyright or acquire a patent for a computer software program or components of a program created by that government entity without statutory authority. In the event that a government entity acquires a patent to a computer software program or component of a program, the data shall be treated as trade secret information pursuant to section 13.37.

Subd. 6. Discoverability of not public data. If a government entity opposes discovery of government data or release of data pursuant to court order on the grounds that the data are classified as not public, the party that seeks access to the data may bring before the appropriate presiding judicial officer, arbitrator, or administrative law judge an action to compel discovery or an action in the nature of an action to compel discovery.

The presiding officer shall first decide whether the data are discoverable or releasable pursuant to the rules of evidence and of criminal, civil, or administrative procedure appropriate to the action.

If the data are discoverable the presiding officer shall decide whether the benefit to the party seeking access to the data outweighs any harm to the confidentiality interests of the entity maintaining the data, or of any person who has provided the data or who is the subject of the data, or to the privacy interest of an individual identified in the data. In making the decision, the presiding officer shall consider whether notice to the subject of the data is warranted and, if warranted, what type of notice must be given. The presiding officer may fashion and issue any protective orders necessary to assure proper handling of the data by the parties. If the data are a videotape of a child victim or alleged victim alleging, explaining, denying, or describing an act of physical or sexual abuse, the presiding officer shall consider the provisions of section 611A.90, subdivision 2, paragraph (b).

Subd. 7. Data transferred to archives. When government data that is classified as not public by this chapter or any other statute, including private data on decedents and confidential data on decedents, is physically transferred to the state archives, the data shall no longer be classified as not public and access to and use of the data shall be governed by section 138.17.

Subd. 8. Change to classification of data not on individuals. Except for security information, nonpublic and protected nonpublic data shall become public either ten years after the creation of the data by the government entity or ten years after the data was received or collected by any governmental entity unless the responsible authority for the originating or custodial entity for the data reasonably determines that, if the data were made available to the public or to the data subject, the harm to the public or to a data subject would outweigh the benefit to the public or to the data subject. If the responsible authority denies access to the data, the person denied access may challenge the denial by bringing an action in district court seeking release of the data. The action shall be brought in the district court located in the county where the data are being maintained, or, in the case of data maintained by a state agency, in any county. The data in dispute shall be examined by the court in camera. In deciding whether or not to release the data, the court shall consider the benefits and harms in the same manner as set forth above. The court shall make a written statement of findings in support of its decision.

Subd. 9. Effect of changes in classification of data. Unless otherwise expressly provided by a particular statute, the classification of data is determined by the law applicable to the data at the time a request for access to the data is made, regardless of the data's classification at the time it was collected, created, or received.

Subd. 10. Costs for providing copies of data. Money collected by a responsible authority in a state agency for the actual cost to the agency of providing copies or electronic transmittal of government data is appropriated to the agency and added to the appropriations from which the costs were paid.

Subd. 11. Treatment of data classified as not public; public meetings. Not public data may be discussed at a meeting open to the public to the extent provided in section 13D.05.

Subd. 12. Pleadings. Pleadings, as defined by court rule, served by or on a government entity, are public data to the same extent that the data would be public if filed with the court.

13.04. Rights of subjects of data

Subdivision 1. Type of data. The rights of individuals on whom the data is stored or to be stored shall be as set forth in this section.

Subd. 2. Tennessen warning. An individual asked to supply private or confidential data concerning the individual shall be informed of: (a) the purpose and intended use of the requested data within the collecting government entity; (b) whether the individual may refuse or is legally required to supply the requested data; (c) any known consequence arising from supplying or refusing to supply private or confidential data; and (d) the identity of other persons or entities authorized by state or federal law to receive the data. This requirement shall not apply when an individual is asked to supply investigative data, pursuant to section 13.82, subdivision 7, to a law enforcement officer.

Subd. 3. Access to data by individual. Upon request to a responsible authority, an individual shall be informed whether the individual is the subject of stored data on individuals, and whether it is classified as public, private or confidential. Upon further request, an individual who is the subject of stored private or public data on individuals shall be shown the data without any charge and, if desired, shall be informed of the content and meaning of that data. After an individual has been shown the private data and informed of its meaning, the data need not be disclosed to that individual for six months thereafter unless a dispute or action pursuant to this section is pending or additional data on the individual has been collected or created. The responsible authority shall provide copies of the private or public data upon request by the individual subject of the data. The responsible authority may require the requesting person to pay the actual costs of making, certifying, and compiling the copies.

The responsible authority shall comply immediately, if possible, with any request made pursuant to this subdivision, or within ten days of the date of the request, excluding Saturdays, Sundays and legal holidays, if immediate compliance is not possible.

Subd. 4. 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.

The determination of the responsible authority may be appealed pursuant to the provisions of the Administrative Procedure Act relating to contested cases. Upon receipt of an appeal by an individual, the commissioner shall, before issuing the order and notice of a contested case hearing required by 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 or issue the order and notice of hearing.

(b) Data on individuals that have been successfully challenged by an individual must be completed, corrected, or destroyed by a state agency, political subdivision, or statewide system without regard to the requirements of section 138.17.

After completing, correcting, or destroying successfully challenged data, a government entity may retain a copy of the commissioner of administration's order issued under chapter 14 or, if no order were issued, a summary of the dispute between the parties that does not contain any particulars of the successfully challenged data.

13.05. Duties of responsible authority

Subdivision 1. Public document of data categories. The responsible authority shall prepare a public document containing the authority's name, 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 authority's government entity. Forms used to collect private and confidential data shall be included in the public document. Beginning August 1, 1977 and annually thereafter, the responsible authority shall update the public document and make any changes necessary to maintain the accuracy of the document. The document shall be available from the responsible authority to the public in accordance with the provisions of sections 13.03 and 15.17.

Subd. 2. Copies to commissioner. The commissioner may require responsible authorities to submit copies of the public document required in subdivision 1, and may request additional information relevant to data collection practices, policies and procedures.

Subd. 3. General standards for collection and storage. Collection and storage of all data on individuals and the use and dissemination of private and confidential data on individuals shall be limited to that necessary for the administration and management of programs specifically authorized by the legislature or local governing body or mandated by the federal government.

Subd. 4. Limitations on collection and use of data. Private or confidential data on an individual shall not be collected, stored, used, or disseminated by government entities for any purposes other than those stated to the individual at the time of collection in accordance with section 13.04, except as provided in this subdivision.

(a) Data collected prior to August 1, 1975, and which have not been treated as public data, may be used, stored, and disseminated for the purposes for which the data was originally collected or for purposes which are specifically approved by the commissioner as necessary to public health, safety, or welfare.

(b) Private or confidential data may be used and disseminated to individuals or entities specifically authorized access to that data by state, local, or federal law enacted or promulgated after the collection of the data.

(c) Private or confidential data may be used and disseminated to individuals or entities subsequent to the collection of the data when the responsible authority maintaining the data has requested approval for a new or different use or dissemination of the data and that request has been specifically approved by the commissioner as necessary to carry out a function assigned by law.

(d) Private data may be used by and disseminated to any person or entity if the individual subject or subjects of the data have given their informed consent. Whether a data subject has given informed consent shall be determined by rules of the commissioner. The format for informed consent is as follows, unless otherwise prescribed by the HIPAA, Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82, 461 (2000) (to be codified as Code of Federal Regulations, title 45, section 164): 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 entity to disclose information about the individual to an insurer or its authorized representative, unless the statement is:

(1) in plain language;

(2) dated;

(3) specific in designating the particular persons or agencies the data subject is authorizing to disclose information about the data subject;

(4) specific as to the nature of the information the subject is authorizing to be disclosed;

(5) specific as to the persons or entities to whom the subject is authorizing information to be disclosed;

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

(7) specific as to its expiration date which should be within a reasonable period of time, not to exceed one year except in the case of authorizations given in connection with applications for (i) life insurance or noncancelable or guaranteed renewable health insurance and identified as such, two years after the date of the policy or (ii) medical assistance under chapter 256B or MinnesotaCare under chapter 256L, which shall be ongoing during all terms of eligibility, for individual education plan health-related services provided by a school district under section 125A.21, subdivision 2.

The responsible authority may require a person requesting copies of data under this paragraph to pay the actual costs of making, certifying, and compiling the copies.

(e) Private or confidential data on an individual may be discussed at a meeting open to the public to the extent provided in section 13D.05.

Subd. 5. Data protection. The responsible authority shall (1) establish procedures to assure that all data on individuals is accurate, complete, and current for the purposes for which it was collected; and (2) establish appropriate security safeguards for all records containing data on individuals.

Subd. 6. Contracts. Except as provided in section 13.46, subdivision 5, in any contract between a government entity subject to this chapter and any person, when the contract requires that data on individuals be made available to the contracting parties by the government entity, that data shall be administered consistent with this chapter. A contracting party shall maintain the data on individuals which it received according to the statutory provisions applicable to the data.

Subd. 7. Preparation of summary data. The use of summary data derived from private or confidential data on individuals under the jurisdiction of one or more responsible authorities is permitted. Unless classified pursuant to section 13.06, another statute, or federal law, summary data is public. The responsible authority shall prepare summary data from private or confidential data on individuals upon the request of any person if the request is in writing and the cost of preparing the summary data is borne by the requesting person. The responsible authority may delegate the power to prepare summary data (1) to the administrative officer responsible for any central repository of summary data; or (2) to a person outside of the entity if the person's purpose is set forth, in writing, and the person agrees not to disclose, and the entity reasonably determines that the access will not compromise private or confidential data on individuals.

Subd. 8. Publication of access procedures. The responsible authority shall prepare a public document setting forth in writing the rights of the data subject pursuant to section 13.04 and the specific procedures in effect in the government entity for access by the data subject to public or private data on individuals.

Subd. 9. Intergovernmental access of data. A responsible authority shall allow another responsible authority access to data classified as not public only when the access is authorized or required by statute or federal law. An entity that supplies government data under this subdivision may require the requesting entity to pay the actual cost of supplying the data.

Subd. 10. International dissemination. No state agency or political subdivision shall transfer or disseminate any private or confidential data on individuals to the private international organization known as Interpol, except through the Interpol-United States National Central Bureau, United States Department of Justice.

Subd. 11. Privatization.

(a) If a government entity enters into a contract with a private person to

perform any of its functions, the government entity shall include in the contract terms that make it clear that all of the data created, collected, received, stored, used, maintained, or disseminated by the private person in performing those functions is subject to the requirements of this chapter and that the private person must comply with those requirements as if it were a government entity. The remedies in section 13.08 apply to the private person under this subdivision.

(b) This subdivision does not create a duty on the part of the private person to provide access to public data to the public if the public data are available from the government entity, except as required by the terms of the contract.

Subd. 12. Identification or justification. Unless specifically authorized by statute, government entities may not require persons to identify themselves, state a reason for, or justify a request to gain access to public government data. A person may be asked to provide certain identifying or clarifying information for the sole purpose of facilitating access to the data.

Subd. 13. Data practices compliance official. By December 1, 2000, each responsible authority or other appropriate authority in every government entity shall appoint or designate an employee of the government entity to act as the entity's data practices compliance official. The data practices compliance official is the designated employee of the government entity to whom persons may direct questions or concerns regarding problems in obtaining access to data or other data practices problems. The responsible authority may be the data practices compliance official.

13.055. State agencies; disclosure of breach in security

Subdivision 1. Definitions. For purposes of this section, the following terms have the meanings given to them.

(a) "Breach of the security of the data" means unauthorized acquisition of data maintained by a state agency that compromises the security and classification of the data. Good faith acquisition of government data by an employee, contractor, or agent of a state agency for the purposes of the state agency is not a breach of the security of the data, if the government data is not provided to an unauthorized person.

(b) "Contact information" means either name and mailing address or name and e-mail address for each individual who is the subject of data maintained by the state agency.

(c) "Unauthorized acquisition" means that a person has obtained government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes.

(d) "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.

Subd. 2. Notice to individuals. A state agency that collects, creates, receives, maintains or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach. Notification must be made to any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with (1) the legitimate needs of a law enforcement agency as provided in subdivision 3; or (2) any measures necessary to determine the scope of the breach and restore the reasonable security of the data.

Subd. 3. Delayed notice. The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede an active criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

Subd. 4. Method of notice. Notice under this section may be provided by one of the following methods:

(a) written notice by first class mail to each affected individual;

(b) electronic notice to each affected individual, if the notice provided is consistent with the provisions regarding electronic records and signatures as set forth in United States Code, title 15, section 7001; or

(c) substitute notice, if the state agency demonstrates that the cost of providing the written notice required by paragraph (a) would exceed $250,000, or that the affected class of individuals to be notified exceeds 500,000, or the state agency does not have sufficient contact information. Substitute notice consists of all of the following:

(i) e-mail notice if the state agency has an e-mail address for the affected individuals;

(ii) conspicuous posting of the notice on the Web site page of the state agency, if the state agency maintains a Web site; and

(iii) notification to major media outlets that reach the general public.

Subd. 5. Coordination with consumer reporting agencies. If the state agency discovers circumstances requiring notification under this section of more than 1,000 individuals at one time, the state agency must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

13.06. Temporary classification

Subdivision 1. Application to commissioner. Notwithstanding the provisions of section 13.03, the responsible authority of a government entity may apply to the commissioner for permission to classify data or types of data on individuals as private or confidential, or data not on individuals as nonpublic or protected nonpublic, for its own use and for the use of other similar government entities on a temporary basis until a proposed statute can be acted upon by the legislature. The application for temporary classification is public.

Upon the filing of an application for temporary classification, the data which is the subject of the application shall be deemed to be classified as set forth in the application for a period of 45 days, or until the application is disapproved, rejected, or granted by the commissioner, whichever is earlier.

If the commissioner determines that an application has been submitted for purposes not consistent with this section, the commissioner may immediately reject the application, give notice of that rejection to the applicant, and return the application. When the applicant receives the notice of rejection from the commissioner, the data which was the subject of the application shall have the classification it had before the application was submitted to the commissioner.

Subd. 2. Contents of application for private or confidential data. An application for temporary classification of data on individuals shall include and the applicant shall have the burden of clearly establishing that no statute currently exists which either allows or forbids classification as private or confidential; and either

(a) that data similar to that for which the temporary classification is sought has been treated as either private or confidential by other government entities, and by the public; or

(b) that a compelling need exists for immediate temporary classification, which if not granted could adversely affect the public interest or the health, safety, well being or reputation of the data subject.

Subd. 3. Contents of application for nonpublic or nonpublic protected data. An application for temporary classification of government data not on individuals shall include and the applicant shall have the burden of clearly establishing that no statute currently exists which either allows or forbids classification as nonpublic or protected nonpublic; and either

(a) that data similar to that for which the temporary classification is sought has been treated as nonpublic or protected nonpublic by other government entities, and by the public; or

(b) public access to the data would render unworkable a program authorized by law; or

(c) that a compelling need exists for immediate temporary classification, which if not granted could adversely affect the health, safety or welfare of the public.

Subd. 4. Procedure when classification affects others. If the commissioner determines that an application for temporary classification involves data which would reasonably be classified in the same manner by all government entities similar to the one which made the application, the commissioner may approve or disapprove the classification for data of the kind which is the subject of the application for the use of all government entities similar to the applicant. On deeming this approach advisable, the commissioner shall provide notice of the proposed action by publication in the State Register within ten days of receiving the application. Within 30 days after publication in the State Reg-

ister an affected government entity or the public may submit comments on the commissioner's proposal. The commissioner shall consider any comments received when granting or denying a classification for data of the kind which is the subject of the application, for the use of all government entities similar to the applicant. Within 45 days after the close of the period for submitting comment, the commissioner shall grant or disapprove the application. Applications processed under this subdivision shall be either approved or disapproved by the commissioner within 90 days of the receipt of the application. For purposes of subdivision 1, the data which is the subject of the classification shall be deemed to be classified as set forth in the application for a period of 90 days, or until the application is disapproved or granted by the commissioner, whichever is earlier. If requested in the application, or determined to be necessary by the commissioner, the data in the application shall be so classified for all government entities similar to the applicant until the application is disapproved or granted by the commissioner, whichever is earlier. Proceedings after the grant or disapproval shall be governed by the provisions of subdivision 5.

Subd. 5. Determination. The commissioner shall either grant or disapprove the application for temporary classification within 45 days after it is filed. On disapproving an application, the commissioner shall set forth in detail reasons for the disapproval, and shall include a statement of belief as to what classification is appropriate for the data which is the subject of the application. Twenty days after the date of the commissioner's disapproval of an application, the data which is the subject of the application shall become public data, unless the responsible authority submits an amended application for temporary classification which requests the classification deemed appropriate by the commissioner in the statement of disapproval or which sets forth additional information relating to the original proposed classification. Upon the filing of an amended application, the data which is the subject of the amended application shall be deemed to be classified as set forth in the amended application for a period of 20 days or until the amended application is granted or disapproved by the commissioner, whichever is earlier. The commissioner shall either grant or disapprove the amended application within 20 days after it is filed. Five working days after the date of the commissioner's disapproval of the amended application, the data which is the subject of the application shall become public data. No more than one amended application may be submitted for any single file or system.

If the commissioner grants an application for temporary classification, it shall become effective immediately, and the complete record relating to the application shall be submitted to the attorney general, who shall review the classification as to form and legality. Within 25 days, the attorney general shall approve the classification, disapprove a classification as confidential but approve a classification as private, or disapprove the classification. If the attorney general disapproves a classification, the data which is the subject of the classification shall become public data five working days after the date of the attorney general's disapproval.

Subd. 6. Repealed by Laws 1995, c. 259, art. 1, § 62.

Subd. 7. Legislative consideration of temporary classifications; expiration. On or before January 15 of each year, the commissioner shall submit all temporary classifications in effect on January 1 in bill form to the legislature. The temporary classification expires June 1 of the year following its submission to the legislature.

13.07. Duties of commissioner

The commissioner shall promulgate rules, in accordance with the rulemaking procedures in the Administrative Procedure Act which shall apply to government entities to implement the enforcement and administration of this chapter. The rules shall not affect section 13.04, relating to rights of subjects of data. Prior to the adoption of rules authorized by this section the commissioner shall give notice to all state agencies and political subdivisions in the same manner and in addition to other parties as required by section 14.06 of the date and place of hearing, enclosing a copy of the rules to be adopted.

13.072. Opinions by the commissioner

Subdivision 1. Opinion; when required.

(a) Upon request of a government entity, the commissioner may give a written opinion on any question relating to public access to government data, rights of subjects of data, or classification of data under this chapter or other Minnesota statutes governing government data practices. Upon request of any person who disagrees with a determination regarding data practices made by a government entity, the commissioner may give a written opinion regarding the person's rights as a subject of government data or right to have access to government data.

(b) Upon request of a body subject to chapter 13D, the commissioner may give a written opinion on any question relating to the body's duties under chapter 13D. Upon request of a person who disagrees with the manner in which members of a governing body perform their duties under chapter 13D, the commissioner may give a written opinion on compliance with chapter 13D. A governing body or person requesting an opinion under this paragraph must pay the commissioner a fee of $200. Money received by the commissioner under this paragraph is appropriated to the commissioner for the purposes of this section.

(c) If the commissioner determines that no opinion will be issued, the commissioner shall give the government entity or body subject to chapter 13D or person requesting the opinion notice of the decision not to issue the opinion within five days of receipt of the request. If this notice is not given, the commissioner shall issue an opinion within 20 days of receipt of the request.

(d) For good cause and upon written notice to the person requesting the opinion, the commissioner may extend this deadline for one additional 30-day period. The notice must state the reason for extending the deadline. The government entity or the members of a body subject to chapter 13D must be provided a reasonable opportunity to explain the reasons for its decision regarding the data or how they perform their duties under chapter 13D. The commissioner or the government entity or body subject to chapter 13D may choose to give notice to the subject of the data concerning the dispute regarding the data or compliance with chapter 13D.

(e) This section does not apply to a determination made by the commissioner of health under section 13.3805, subdivision 1, paragraph (b), or 144.6581.

(f) A written opinion issued by the attorney general shall take precedence over an opinion issued by the commissioner under this section.

Subd. 2. Effect. Opinions issued by the commissioner under this section are not binding on the government entity or members of a body subject to chapter 13D whose data or performance of duties is the subject of the opinion, but an opinion described in subdivision 1, paragraph (a), must be given deference by a court in a proceeding involving the data. The commissioner shall arrange for public dissemination of opinions issued under this section. This section does not preclude a person from bringing any other action under this chapter or other law in addition to or instead of requesting a written opinion. A government entity, members of a body subject to chapter 13D, or person that acts in conformity with a written opinion of the commissioner issued to the government entity, members, or person or to another party is not liable for compensatory or exemplary damages or awards of attorneys fees in actions under section 13.08 or for a penalty under section 13.09 or for fines, awards of attorney fees, or any other penalty under chapter 13D. A member of a body subject to chapter 13D is not subject to forfeiture of office if the member was acting in reliance on an opinion.

Subd. 3. Repealed by Laws 1997, 1st Sp., c. 3, § 47.

Subd. 4. Data submitted to commissioner. A government entity may submit not public data to the commissioner for the purpose of requesting or responding to a person's request for an opinion. Government data submitted to the commissioner by a government entity or copies of government data submitted by other persons have the same classification as the data have when held by the government entity. If the nature of the opinion is such that the release of the opinion would reveal not public data, the commissioner may issue an opinion using pseudonyms for individuals. Data maintained by the commissioner, in the record of an opinion issued using pseudonyms that would reveal the identities of individuals protected by the use of the pseudonyms, are private data on individuals.

13.073. Public information policy training program

Subdivision 1. Establishment. The commissioner may establish a program for training state and local government officials and employees on public information policy, including government data practices laws and official records and records management statutes. The program may provide for the development of broad-based expertise within state and local government entities. The program components may include basic training, specific training for specialized service sectors, and policy analysis and support.

Subd. 2. General provisions. The commissioner may publicize the development and implementation of the training program under this section and

seek input from state and local government entities. The commissioner may prepare a training guide that includes an overview of the training program and its components.

Subd. 3. Basic training. The basic training component should be designed to meet the basic information policy needs of all government employees and public officials with a focus on key data practices laws and procedures that apply to all government entities. The commissioner should design the basic training component in a manner that minimizes duplication of the effort and cost for government entities to provide basic training. The commissioner may develop general programs and materials for basic training such as video presentations, data practices booklets, and training guides. The commissioner may assist state and local government entities in developing training expertise within their own entities and offer assistance for periodic training sessions for this purpose.

Subd. 4. Sector-specific training.

(a) The sector-specific training component should be designed to provide for the development of specific expertise needed to deal with information policy issues within a particular service area. Service areas may include government entities such as state agencies, counties, cities, or school districts, or functional areas such as education, human services, child protection, or law enforcement. This component should focus on training individuals who implement or administer data practices and other information policy laws within their government entity.

(b) The commissioner may provide technical assistance and support and help coordinate efforts to develop sector-specific training within different sectors. Elements of sector-specific training should include:

(1) designation, training, and coordination of data practices specialists with responsibility for clarification and resolution of sector-specific information policy issues;

(2) development of telephone hot lines within different sectors for handling information policy inquiries;

(3) development of forums under which individuals with ongoing information policy administrative responsibilities may meet to discuss issues arising within their sectors;

(4) availability of expertise for coaching and consultation on specific issues; and

(5) preparation of publications, including reference guides to materials and resource persons.

Subd. 5. Policy analysis and support. The policy analysis and support component should be designed to address information policy issues at the policy level and to provide ongoing consultation and support regarding major areas of concern with a goal of developing a coherent and coordinated approach to information policy within the state. The commissioner may assist in the development and implementation of information policy and provide a clearinghouse for ideas, information, and resources. The commissioner may review public information policy and identify how that policy can be updated, simplified, and made consistent.

Subd. 6. Preparation of model policies and procedures. The commissioner shall, in consultation with affected government entities, prepare model policies and procedures to assist government entities in complying with the requirements of this chapter that relate to public access to government data and rights of subjects of data. Upon completion of a model for a governmental level, the commissioner shall offer that model for formal adoption by that level of government. Government entities may adopt or reject the model offered by the commissioner. A government entity that adopts the commissioner's model shall notify the commissioner in a form prescribed by the commissioner.

13.08. Civil remedies

Subdivision 1. Action for damages. Notwithstanding section 466.03, a responsible authority or government entity which violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damage as a result of the violation, and the person damaged or a representative in the case of private data on decedents or confidential data on decedents may bring an action against the responsible authority or government entity to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, the government entity shall, in addition, be liable to exemplary damages of not less than $100, nor more than $10,000 for each violation. The state is deemed to have waived any immunity to a cause of action brought under this chapter.

Subd. 2. Injunction. A responsible authority or government entity which violates or proposes to violate this chapter may be enjoined by the district court. The court may make any order or judgment as may be necessary to prevent the use or employment by any person of any practices which violate this chapter.

Subd. 3. Venue. An action filed pursuant to this section may be commenced in the county in which the individual alleging damage or seeking relief resides, or in the county wherein the political subdivision exists, or, in the case of the state, any county.

Subd. 4. Action to compel compliance.

(a) In addition to the remedies provided in subdivisions 1 to 3 or any other law, any aggrieved person seeking to enforce the person's rights under this chapter or obtain access to data may bring an action in district court to compel compliance with this chapter and may recover costs and disbursements, including reasonable attorney's fees, as determined by the court. If the court determines that an action brought under this subdivision is frivolous and without merit and a basis in fact, it may award reasonable costs and attorney fees to the responsible authority. If the court issues an order to compel compliance under this subdivision, the court may impose a civil penalty of up to $300 against the government entity. This penalty is payable to the state general fund and is in addition to damages under subdivision 1. The matter shall be heard as soon as possible. In an action involving a request for government data under section 13.03 or 13.04, the court may inspect in camera the government data in dispute, but shall conduct its hearing in public and in a manner that protects the security of data classified as not public. If the court issues an order to compel compliance under this subdivision, the court shall forward a copy of the order to the commissioner of administration.

(b) In determining whether to assess a civil penalty under this subdivision, the court shall consider whether the government entity has substantially complied with general data practices under this chapter, including but not limited to, whether the government entity has:

(1) designated a responsible authority under section 13.02, subdivision 16;

(2) designated a data practices compliance official under section 13.05, subdivision 13;

(3) prepared the public document that names the responsible authority and describes the records and data on individuals that are maintained by the government entity under section 13.05, subdivision 1;

(4) developed public access procedures under section 13.03, subdivision 2; procedures to guarantee the rights of data subjects under section 13.05, subdivision 8; and procedures to ensure that data on individuals are accurate and complete and to safeguard the data's security under section 13.05, subdivision 5;

(5) sought an oral, written, or electronic opinion from the commissioner of administration related to the matter at issue and acted in conformity with that opinion or acted in conformity with an opinion issued under section 13.072 that was sought by another person; or

(6) provided ongoing training to government entity personnel who respond to requests under this chapter.

(c) The court shall award reasonable attorney fees to a prevailing plaintiff who has brought an action under this subdivision if the government entity that is the defendant in the action was also the subject of a written opinion issued under section 13.072 and the court finds that the opinion is directly related to the cause of action being litigated and that the government entity did not act in conformity with the opinion.

Subd. 5. Immunity from liability. A government entity or person that releases not public data pursuant to an order under section 13.03, subdivision 6 is immune from civil and criminal liability.

Subd. 6. Immunity from liability; personnel settlement. No cause of action may arise as a result of the release of data contained in a termination or personnel settlement agreement if the data were not public data as defined in section 13.02, at the time the agreement was executed but become public data under a law enacted after execution.

13.081. Repealed by Laws 2001, c. 202, § 21

13.09. Penalties

Any person who willfully violates the provisions of this chapter or any rules

adopted under this chapter is guilty of a misdemeanor. Willful violation of this chapter by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.

13.10. Data on decedents

Subdivision 1. Definitions. As used in this chapter:

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

(b) "Private data on decedents" means data which, prior to the death of the data subject, were classified by statute, federal law, or temporary classification as private data.

(c) "Representative of the decedent" means 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 is no surviving spouse or children, the parents of the decedent.

Subd. 2. Classification of data on decedents. Upon the death of the data subject, private data and confidential data shall become, respectively, private data on decedents and confidential data on decedents. Private data on decedents and confidential data on decedents shall become public when ten 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 subdivision, 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 that an individual is not presumed to be dead if readily available data indicate that the individual is still living.

Subd. 3. Rights. Rights conferred by this chapter on individuals who are the subjects of private or confidential data shall, in the case of private data on decedents or confidential data on decedents, be exercised by the representative of the decedent. Nonpublic data concerning a decedent, created or collected after death, are accessible by the representative of the decedent. Nothing in this section may be construed to prevent access to appropriate data by a trustee appointed in a wrongful death action.

Subd. 4. Court review. Any person may bring an action in the district court located in the county where the data is being maintained or, in the case of data maintained by a state agency, in any county, to authorize release of private data on decedents or confidential data on decedents. Individuals clearly identified in the data or the representative of the decedent may be given notice if doing so does not cause an undue delay in hearing the matter and, in any event, shall have standing in the court action. The responsible authority for the data being sought or any interested person may provide information regarding the possible harm or benefit from granting the request. The data in dispute shall be examined by the court in camera. The court may order all or part of the data to be released to the public or to the person bringing the action. In deciding whether or not to release the data, the court shall consider whether the harm to the surviving spouse, children, or next of kin of the decedent, the harm to any other individual identified in the data, or the harm to the public outweighs the benefit to the person bringing the action or the benefit of the public. The court shall make a written statement of findings in support of its decision.

Subd. 5. Adoption records. Notwithstanding any provision of this chapter, adoption records shall be treated as provided in sections 259.53, 259.61, 259.79, and 259.83 to 259.89.

Subd. 6. Retention of data. Nothing in this section may be construed to require retention of government data, including private data on decedents or confidential data on decedents, for periods of time other than those established by the procedures provided in section 138.17, or any other statute.

Computer Data

13.15. Computer data

Subdivision 1. Definitions. As used in this section, the following terms have the meanings given.

(a) Electronic access data. "Electronic access data" means data created, collected, or maintained about a person's access to a government entity's computer for the purpose of:

(1) gaining access to data or information;

(2) transferring data or information; or

(3) using government services.

(b) Cookie. "Cookie" means any data that a government-operated computer electronically places on the computer of a person who has gained access to a government computer.

Subd. 2. Classification of data. Electronic access data are private data on individuals or nonpublic data.

Subd. 3. Notice; refusal to accept cookie.

(a) A government entity that creates, collects, or maintains electronic access data or uses its computer to install a cookie on a person's computer must inform persons gaining access to the entity's computer of the creation, collection, or maintenance of electronic access data or the entity's use of cookies before requiring the person to provide any data about the person to the government entity. As part of that notice, the government entity must inform the person how the data will be used and disseminated, including the uses and disseminations in subdivision 4.

(b) Notwithstanding a person's refusal to accept a cookie on the person's computer, a government entity must allow the person to gain access to data or information, transfer data or information, or use government services by the government entity's computer.

Subd. 4. Use of electronic access data. Electronic access data may be disseminated:

(1) to the commissioner for the purpose of evaluating electronic government services;

(2) to another government entity to prevent unlawful intrusions into government electronic systems; or

(3) as otherwise provided by law.

Political Subdivision Data

13.201. Rideshare data

The following data on participants, collected by the Minnesota department of transportation and the metropolitan council to administer rideshare programs, are classified as private under section 13.02, subdivision 12: residential address and telephone number; beginning and ending work hours; current mode of commuting to and from work; and type of rideshare service information requested.

13.202. Political subdivision data coded elsewhere

Subdivision 1. Scope. The sections referenced in subdivisions 2 to 12 are codified outside this chapter. Those sections classify political subdivision data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. County boards; property tax abatement. Certain data in an application for property tax abatement are classified under section 375.192, subdivision 2.

Subd. 3. Hennepin county.

(a) Records of closed county board meetings. Records of Hennepin county board meetings permitted to be closed under section 383B.217, subdivision 7, are classified under that subdivision.

(b) Medical examiner investigations. Certain data on deceased persons collected or created by the Hennepin county medical examiner are classified under section 383B.225.

Subd. 4. Coroner; inquest data. Certain data collected or created in the course of a coroner's or medical examiner's inquest are classified under sections 390.11, subdivision 7, and 390.32, subdivision 6.

Subd. 5. Solid waste management; collector audit. Data obtained in an audit of a solid waste collector under section 400.08, subdivision 4, are classified under that subdivision.

Subd. 6. 911 emergency telephone service; public utility data. Public utility data and names, addresses, and telephone numbers provided to a 911 system under section 403.07, subdivisions 3 and 4, are classified under those subdivi-

sions.

Subd. 7. Public facilities authority; financial data. Financial information received or prepared by a public facilities authority is classified under section 446A.11, subdivision 11.

Subd. 8. Repealed by Laws 2002, c. 220, art. 10, § 40, eff. July 1, 2002.

Subd. 9. Municipal Rights.

(a) Self-insurer claims. Disclosure of information about individual claims filed by the employees of a municipality which is a self-insurer is governed by section 471.617, subdivision 5.

(b) Meetings of governing bodies. Treatment of data discussed at meetings of governing bodies is governed by section 13D.05.

(c) Job evaluation system reports. Treatment of reports containing the results of job evaluation systems is governed by section 471.995.

(d) Pay equity compliance. Implementation reports of equitable compensation plans are classified by section 471.9981, subdivision 5b.

Subd. 10. Capital intensive public service proposals and negotiation documents. Proposals received from vendors, and all government data received from vendors or generated by a municipality relating to negotiations with vendors, for capital intensive public services are classified under section 471A.03, subdivision 3.

Subd. 11. Metropolitan government.

(a) Affirmative action plans. Treatment of data relating to metropolitan agency affirmative action plans is governed by section 473.143, subdivisions 5 and 7.

(b) Contracts for management services. Data relating to compensation of personnel who work under a management service contract are classified by section 473.405, subdivision 12.

(c) Arena acquisition. Certain data in connection with a decision whether to acquire a sports arena are classified under section 473.598, subdivision 4.

(d) Airports commission. Certain airline data submitted to the metropolitan airports commission in connection with the issuance of revenue bonds are classified under section 473.6671, subdivision 3.

(e) Solid waste landfill fee. Information obtained from the operator of a mixed municipal solid waste disposal facility under section 473.843 is classified under section 473.843, subdivision 4.

Subd. 12. Public indebtedness; municipal obligation register data. Information contained in a register with respect to the ownership of certain municipal obligations is classified under section 475.55, subdivision 6.

13.203. Service cooperative claims data

Claims experience and all related information received from carriers and claims administrators participating in a group health or dental plan, including any long-term disability plan, offered through the Minnesota service cooperatives to Minnesota school districts and other political subdivisions, and survey information collected from employees and employers participating in these plans and programs, except when the executive director of a Minnesota service cooperative determines that release of the data will not be detrimental to the plan or program, are classified as nonpublic data not on individuals.

13.30. Renumbered 13.393 in St.2000

13.31. Renumbered 13.462 in St.2000

Educational Data

13.319. Education data coded elsewhere

Subdivision 1. Scope. The sections referred to in subdivisions 2 to 6 are codified outside this chapter. Those sections classify education data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. Grants to service provider programs; abused children service. Treatment of data related to grants for programs which provide abused children services is governed by section 119A.21, subdivision 4.

Subd. 3. Program services. Data on individuals receiving services under certain programs administered by the Department of Education are classified under section 119A.50, subdivision 2.

Subd. 4. Energy programs. Treatment of data on individuals applying for benefits or services under energy programs is governed by section 216C.266.

Subd. 5. Renumbered 13.461, subd. 30, in St.2005 Supp.

Subd. 6. Lead abatement program; testing and evaluation. Treatment of data relating to testing under the lead abatement program is governed by section 144.9512, subdivision 8.

Subd. 7. Repealed by Laws 2004, c. 290, § 39.

13.32. Educational data

Subdivision 1. Definitions. As used in this section:

(a) "Educational data" means data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution which relates to a student.

Records of instructional personnel which are in the sole possession of the maker thereof and are not accessible or revealed to any other individual except a substitute teacher, and are destroyed at the end of the school year, shall not be deemed to be government data.

Records of a law enforcement unit of a public educational agency or institution which are maintained apart from education data and are maintained solely for law enforcement purposes, and are not disclosed to individuals other than law enforcement officials of the jurisdiction are not educational data; provided, that education records maintained by the educational agency or institution are not disclosed to the personnel of the law enforcement unit. The University of Minnesota police department is a law enforcement agency for purposes of section 13.82 and other sections of Minnesota Statutes dealing with law enforcement records. Records of organizations providing security services to a public educational agency or institution must be administered consistent with section 13.861.

Records relating to a student who is employed by a public educational agency or institution which are made and maintained in the normal course of business, relate exclusively to the individual in that individual's capacity as an employee, and are not available for use for any other purpose are classified pursuant to section 13.43.

(b) "Juvenile justice system" includes criminal justice agencies and the judiciary when involved in juvenile justice activities.

(c) "Student" means an individual currently or formerly enrolled or registered, applicants for enrollment or registration at a public educational agency or institution, or individuals who receive shared time educational services from a public agency or institution.

(d) "Substitute teacher" means an individual who performs on a temporary basis the duties of the individual who made the record, but does not include an individual who permanently succeeds to the position of the maker of the record.

Subd. 2. Student health and census data; data on parents.

(a) Health data concerning students, including but not limited to, data concerning immunizations, notations of special physical or mental problems and records of school nurses are educational data. Access by parents to student health data shall be pursuant to section 13.02, subdivision 8.

(b) Pupil census data, including emergency information and family information are educational data.

(c) Data concerning parents are private data on individuals but may be treated as directory information if the same procedures that are used by a school district to designate student data as directory information under subdivision 5 are followed.

Subd. 3. Private data; when disclosure is permitted. Except as provided in subdivision 5, educational data is private data on individuals and shall not be disclosed except as follows:

(a) pursuant to section 13.05;

(b) pursuant to a valid court order;

(c) pursuant to a statute specifically authorizing access to the private data;

(d) to disclose information in health and safety emergencies pursuant to the provisions of United States Code, title 20, section 1232g(b)(1)(I) and Code of Federal Regulations, title 34, section 99.36;

(e) pursuant to the provisions of United States Code, title 20, sections 1232g(b)(1), (b)(4)(A), (b)(4)(B), (b)(1)(B), (b)(3) and Code of Federal Regulations, title 34, sections 99.31, 99.32, 99.33, 99.34, and 99.35;

(f) to appropriate health authorities to the extent necessary to administer immunization programs and for bona fide epidemiologic investigations which the commissioner of health determines are necessary to prevent disease or disability to individuals in the public educational agency or institution in which the investigation is being conducted;

(g) when disclosure is required for institutions that participate in a program under title IV of the Higher Education Act, United States Code, title 20, section 1092;

(h) to the appropriate school district officials to the extent necessary under subdivision 6, annually to indicate the extent and content of remedial instruction, including the results of assessment testing and academic performance at a postsecondary institution during the previous academic year by a student who graduated from a Minnesota school district within two years before receiving the remedial instruction;

(i) to appropriate authorities as provided in United States Code, title 20, section 1232g(b)(1)(E)(ii), if the data concern the juvenile justice system and the ability of the system to effectively serve, prior to adjudication, the student whose records are released; provided that the authorities to whom the data are released submit a written request for the data that certifies that the data will not be disclosed to any other person except as authorized by law without the written consent of the parent of the student and the request and a record of the release are maintained in the student's file;

(j) to volunteers who are determined to have a legitimate educational interest in the data and who are conducting activities and events sponsored by or endorsed by the educational agency or institution for students or former students;

(k) to provide student recruiting information, from educational data held by colleges and universities, as required by and subject to Code of Federal Regulations, title 32, section 216;

(l) to the juvenile justice system if information about the behavior of a student who poses a risk of harm is reasonably necessary to protect the health or safety of the student or other individuals;

(m) with respect to Social Security numbers of students in the adult basic education system, to Minnesota State Colleges and Universities and the Department of Employment and Economic Development for the purpose and in the manner described in section 124D.52, subdivision 7; or

(n) to the commissioner of education for purposes of an assessment or investigation of a report of alleged maltreatment of a student as mandated by section 626.556. Upon request by the commissioner of education, data that are relevant to a report of maltreatment and are from charter school and school district investigations of alleged maltreatment of a student must be disclosed to the commissioner, including, but not limited to, the following:

(1) information regarding the student alleged to have been maltreated;

(2) information regarding student and employee witnesses;

(3) information regarding the alleged perpetrator; and

(4) what corrective or protective action was taken, if any, by the school facility in response to a report of maltreatment by an employee or agent of the school or school district.

Subd. 4. Student's access to private data. A student shall not have the right of access to private data provided in section 13.04, subdivision 3, as to financial records and statements of the student's parents or any information contained therein.

Subd. 4a. Nonpublic school students. Data collected by a public school on a child or parent of a child, whose identity must be reported pursuant to section 120A.24, is private data which:

(1) shall not be designated directory information pursuant to subdivision 5 unless prior written consent is given by the child's parent or guardian; and

(2) may be disclosed only pursuant to subdivision 3, clause (a), (b), (c), or (f).

This provision does not apply to students who receive shared time educational services from a public agency or institution.

Subd. 5. Directory information. Information designated as directory information pursuant to the provisions of United States Code, title 20, section 1232g and Code of Federal Regulations, title 34, section 99.37 which are in effect on July 1, 1993, is public data on individuals. When conducting the directory information designation and notice process required by federal law, an educational agency or institution shall give parents and students notice of the right to refuse to let the agency or institution designate any or all data about the student as directory information. This notice may be given by any means reasonably likely to inform the parents and students of the right.

Subd. 5a. Military recruitment. A secondary institution shall release to military recruiting officers the names, addresses, and home telephone numbers of students in grades 11 and 12 within 60 days after the date of the request, except as otherwise provided by this subdivision. A secondary institution shall give parents and students notice of the right to refuse release of this data to military recruiting officers. Notice may be given by any means reasonably likely to inform the parents and students of the right. Data released to military recruiting officers under this subdivision:

(1) may be used only for the purpose of providing information to students about military service, state and federal veterans' education benefits, and other career and educational opportunities provided by the military; and

(2) shall not be further disseminated to any other person except personnel of the recruiting services of the armed forces.

Subd. 6. Admissions forms; remedial instruction.

(a) Minnesota postsecondary education institutions, for purposes of reporting and research, may collect on the 1986-1987 admissions form, and disseminate to any public educational agency or institution the following data on individuals: student sex, ethnic background, age, and disabilities. The data shall not be required of any individual and shall not be used for purposes of determining the person's admission to an institution.

(b) A school district that receives information under subdivision 3, paragraph (h) from a postsecondary institution about an identifiable student shall maintain the data as educational data and use that data to conduct studies to improve instruction. Public postsecondary systems annually shall provide summary data to the department of education indicating the extent and content of the remedial instruction received in each system during the prior academic year by, and the results of assessment testing and the academic performance of, students who graduated from a Minnesota school district within two years before receiving the remedial instruction. The department shall evaluate the data and annually report its findings to the education committees of the legislature.

(c) This section supersedes any inconsistent provision of law.

Subd. 7. Uses of data. School officials who receive data on juveniles, as authorized under section 260B.171, may use and share that data as provided in section 121A.75. A school district, its agents, and employees who use and share this data in good faith are immune from civil or criminal liability that might otherwise result from their actions.

Subd. 8. Access by juvenile justice system.

(a) Upon request, the following education data shall be disclosed under subdivision 3, clause (i), to the juvenile justice system: a student's full name, home address, telephone number, date of birth; a student's school schedule, daily attendance record, and photographs, if any; and parents' names, home addresses, and telephone numbers.

(b) In addition, the existence of the following data about a student may be disclosed under subdivision 3, clause (i):

(1) use of a controlled substance, alcohol, or tobacco;

(2) assaultive or threatening conduct that could result in dismissal from school under section 121A.45, subdivision 2, clause (b) or (c);

(3) possession or use of weapons or look-alike weapons;

(4) theft; or

(5) vandalism or other damage to property.

Any request for access to data under this paragraph must contain an

explanation of why access to the data is necessary to serve the student.

(c) A principal or chief administrative officer of a school who receives a request to disclose information about a student to the juvenile justice system under paragraph (b) shall, to the extent permitted by federal law, notify the student's parent or guardian by certified mail of the request to disclose information before disclosing the information. If the student's parent or guardian notifies the principal or chief administrative officer within ten days of receiving the certified notice that the parent or guardian objects to the disclosure, the principal or chief administrative officer must not disclose the information. The principal or chief administrative officer must inform the requesting member of the juvenile justice system of the objection.

(d) A principal or chief administrative officer is not required to create data under this subdivision. Information provided in response to a data request under paragraph (b) shall indicate only whether the data described in paragraph (b) exist. The principal or chief administrative officer is not authorized under paragraph (b) to disclose the actual data or other information contained in the student's education record. A principal or chief administrative officer is not required to provide data that are protected by court order. A principal or chief administrative officer must respond to a data request within 14 days if no objection is received from the parent or guardian.

(e) Nothing in this subdivision shall limit the disclosure of educational data pursuant to court order.

(f) A school district, its agents, and employees who provide data in good faith under this subdivision are not liable for compensatory or exemplary damages or an award of attorney fees in an action under section 13.08, or other law, or for a penalty under section 13.09.

(g) Section 13.03, subdivision 4, applies to data that are shared under this subdivision with a government entity. If data are shared with a member of the juvenile justice system who is not a government entity, the person receiving the shared data must treat the data consistent with the requirements of this chapter applicable to a government entity.

(h) A member of the juvenile justice system who falsely certifies a request for data under this section is subject to the penalties under section 13.09.

Subd. 9. Forms. To make a data request under subdivision 8, paragraph (b), a member of the juvenile justice system must use the following form:

REQUEST FOR INFORMATION

Family Educational Rights and Privacy Act/ Minnesota Government Data Practices

Act

DATE/TIME OF REQUEST . . ..

TO: . . ..

(Superintendent of school district

or chief administrative officer of school)

FROM: . . ..

(Requester's name/agency)

STUDENT: . . ..

BASIS FOR REQUEST

. . . Juvenile delinquency investigation/prosecution

. . . Child protection assessment/investigation

. . . Investigation/filing of CHIPS or delinquency petition

REASON FOR REQUEST (requester must describe why information regarding existence

of the data marked below is necessary to effectively serve the student) . . ...

. . ..

. . ..

. . ..

RESPONSE TO REQUEST

The school must indicate whether it has data on the student that document

any activity or behavior marked by the requester.

INFORMATION REQUESTED (mark all that apply)

RESPONSE

Indicate whether you have data that document the student's: (yes or no)

. . .. use of a controlled substance, alcohol, or tobacco

. . .. assaultive or threatening conduct as defined in Minnesota

. . .. Statutes, section 13.32, subdivision 8

. . .. possession or use of weapons or look alike weapons

. . .

. . .. theft

. . .. vandalism and damage to property

. . .

CERTIFICATION: The undersigned certifies that the undersigned is a member of the juvenile justice system. The requested data are needed by the juvenile justice system so it may effectively serve, prior to adjudication, the student whose records are released. The undersigned will not disclose the information received to any other party, except as provided under state law, without prior written consent as required by Code of Federal Regulations, title 34, section 99.38(b). The undersigned further certifies that the undersigned understands that by signing this request, the undersigned is subject to the penalties in Minnesota Statutes, section 13.09.

. . ..

Signature/Title

Subd. 10. Education records; child with disability. Nothing in this chapter shall be construed as limiting the frequency of inspection of the educational records of a child with a disability by the child's parent or guardian or by the child upon the child reaching the age of majority. An agency or institution may not charge a fee to search for or to retrieve the educational records. An agency or institution that receives a request for copies of the educational records of a child with a disability may charge a fee that reflects the costs of reproducing the records except when to do so would impair the ability of the child's parent or guardian, or the child who has reached the age of majority, to exercise their right to inspect and review those records.

13.321. Prekindergarten-grade 12 educational data coded elsewhere

Subdivision 1. Scope. The sections referred to in subdivisions 2 to 10 are codified outside this chapter. Those sections classify prekindergarten to grade 12 educational data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. Curriculum and assessment; testing data. Data sharing involving the statewide testing and reporting system is governed by sections 120B.30, subdivision 3, and 120B.31, subdivision 4.

Subd. 2a. School accountability. Certain school accountability data are governed by section 120B.36, subdivisions 1, paragraph (e), and 2.

Subd. 3. Disposition orders received by schools. Access to disposition orders received by schools is governed by section 121A.75.

Subd. 4. Student rights, responsibilities, and behavior.

(a) Immunization data. Data sharing involving immunization records is governed by section 121A.15, subdivision 7.

(b) Developmental screening. Data collected in early childhood developmental screening programs are classified under section 121A.18.

(c) Exclusions and expulsions. Data sharing involving exclusions and expulsions is classified under section 121A.53.

Subd. 5. Teachers; license reporting. Data on certain teacher discharges and resignations reported under section 122A.20 are classified under that section.

Subd. 6. School district powers; energy efficiency projects. Data involving

energy efficiency project contracts are governed by section 123B.65, subdivision 10.

Subd. 7. Education programs.

(a) School readiness program. Data on a child participating in a school readiness program are classified under section 124D.15, subdivision 9.

(b) Renumbered 13.461, subd. 31, in St.2005 Supp.

(c) Performance tracking system. Data sharing related to the performance tracking system is governed by section 124D.52.

Subd. 8. Special education.

(a) Third party payment. Disclosure of student data to health plan companies is governed by section 125A.21, subdivision 7.

(b) Agency access. Agency access to data about a child with a disability is governed by section 125A.23.

(c) Interagency early intervention committees. Data sharing involving interagency early intervention committees is governed by sections 125A.027, subdivision 1, and 125A.30.

Subd. 9. High school league. Data involving the high school league are governed by section 128C.17.

Subd. 10. Teacher data from value-added assessment model. Data on individual teachers generated from a value-added assessment model are governed under section 120B.362.

13.3215. University of Minnesota data

Claims experience and all related information received from carriers and claims administrators participating in a University of Minnesota group health, dental, life, or disability insurance plan or the University of Minnesota workers' compensation program, and survey information collected from employees or students participating in these plans and programs, except when the university determines that release of the data will not be detrimental to the plan or program, are classified as nonpublic data not on individuals pursuant to section 13.02, subdivision 9.

13.322. Postsecondary education data coded elsewhere

Subdivision 1. Scope. The sections referred to in subdivisions 2 to 4 are codified outside this chapter. Those sections classify higher education data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. Public postsecondary education; immunization files. Data sharing of immunization records is governed by section 135A.14, subdivision 4.

Subd. 3. Higher education services office.

(a) General. Data sharing involving the higher education services office and other institutions is governed by section 136A.05.

(b) Student financial aid. Data collected and used by the higher education services office on applicants for financial assistance are classified under section 136A.162.

(c) Minnesota college savings plan data. Account owner data, account data, and data on beneficiaries of accounts under the Minnesota college savings plan are classified under section 136G.05, subdivision 10.

(d) School financial records. Financial records submitted by schools registering with the higher education services office are classified under section 136A.64.

Subd. 4. Private career schools; inspection. Data obtained from an inspection of the financial records of a school are governed by section 141.30.

13.33. Renumbered 13.601, subd. 2, in St.2000

General Data

13.34. Examination data

Data consisting solely of testing or examination materials, or scoring keys used solely to determine individual qualifications for appointment or promotion in public service, or used to administer a licensing examination, or academic examination, the disclosure of which would compromise the objectivity or fairness of the testing or examination process are classified as nonpublic, except pursuant to court order. Completed versions of personnel, licensing, or academic examinations shall be accessible to the individual who completed the examination, unless the responsible authority determines that access would compromise the objectivity, fairness, or integrity of the examination process. Notwithstanding section 13.04, the responsible authority shall not be required to provide copies of completed examinations or answer keys to any individual who has completed an examination.

13.35. Federal contracts data

To the extent that a federal agency requires it as a condition for contracting with a state agency or political subdivision, all government data collected and maintained by the state agency or political subdivision because that agency contracts with the federal agency are classified as either private or nonpublic depending on whether the data are data on individuals or data not on individuals.

13.355. Social security numbers

Subdivision 1. General. The social security numbers of individuals collected or maintained by a state agency, statewide system, or political subdivision are private data on individuals, except to the extent that access to the social security number is specifically authorized by law.

Subd. 2. County recorder or registrar of titles. Subdivision 1 does not apply to social security numbers that appear in documents or records filed or recorded with the county recorder or registrar of titles, other than documents filed under section 600.23.

13.36. Renumbered 13.87, subd. 2, in St.2000

13.37. General nonpublic data

Subdivision 1. Definitions. As used in this section, the following terms have the meanings given them.

(a) "Security information" means government data the disclosure of which would be likely to substantially jeopardize the security of information, possessions, individuals or property against theft, tampering, improper use, attempted escape, illegal disclosure, trespass, or physical injury. "Security information" includes crime prevention block maps and lists of volunteers who participate in community crime prevention programs and their home addresses and telephone numbers.

(b) "Trade secret information" means government data, including a formula, pattern, compilation, program, device, method, technique or process (1) that was supplied by the affected individual or organization, (2) that is the subject of efforts by the individual or organization that are reasonable under the circumstances to maintain its secrecy, and (3) that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.

(c) "Labor relations information" means management positions on economic and noneconomic items that have not been presented during the collective bargaining process or interest arbitration, including information specifically collected or created to prepare the management position.

(d) "Parking space leasing data" means the following government data on an applicant for, or lessee of, a parking space: residence address, home telephone number, beginning and ending work hours, place of employment, work telephone number, and location of the parking space.

Subd. 2. Classification. The following government data is classified as nonpublic data with regard to data not on individuals, pursuant to section 13.02, subdivision 9, and as private data with regard to data on individuals, pursuant to section 13.02, subdivision 12: Security information; trade secret information; sealed absentee ballots prior to opening by an election judge; sealed bids, including the number of bids received, prior to the opening of the bids; parking space leasing data; and labor relations information, provided that specific labor

relations information which relates to a specific labor organization is classified as protected nonpublic data pursuant to section 13.02, subdivision 13.

Subd. 3. Data dissemination.

(a) Crime prevention block maps and names, home addresses, and telephone numbers of volunteers who participate in community crime prevention programs may be disseminated to volunteers participating in crime prevention programs. The location of a National Night Out event is public data.

(b) The responsible authority of a government entity in consultation with the appropriate chief law enforcement officer, emergency manager, or public health official, may make security information accessible to any person, entity, or the public if the government entity determines that the access will aid public health, promote public safety, or assist law enforcement.

13.38. Renumbered 13.3805, subd. 1, in St.2000

Health and Medical Data

13.3805. Public health data

Subdivision 1. Health data generally.

(a) Definitions. As used in this subdivision:

(1) "Commissioner" means the commissioner of health.

(2) "Health data" means data on individuals created, collected, received, or maintained by the department of health, political subdivisions, or statewide systems relating to the identification, description, prevention, and control of disease or as part of an epidemiologic investigation the commissioner designates as necessary to analyze, describe, or protect the public health.

(b) Data on individuals.

(1) Health data are private data on individuals. Notwithstanding section 13.05, subdivision 9, health data may not be disclosed except as provided in this subdivision and section 13.04.

(2) The commissioner or a local board of health as defined in section 145A.02, subdivision 2, may disclose health data to the data subject's physician as necessary to locate or identify a case, carrier, or suspect case, to establish a diagnosis, to provide treatment, to identify persons at risk of illness, or to conduct an epidemiologic investigation.

(3) With the approval of the commissioner, health data may be disclosed to the extent necessary to assist the commissioner to locate or identify a case, carrier, or suspect case, to alert persons who may be threatened by illness as evidenced by epidemiologic data, to control or prevent the spread of serious disease, or to diminish an imminent threat to the public health.

(c) Health summary data. Summary data derived from data collected under section 145.413 may be provided under section 13.05, subdivision 7.

Subd. 2. Huntington's disease data. All data created, collected, received, or maintained by the commissioner of health on individuals relating to genetic counseling services for Huntington's Disease provided by the department of health are private data on individuals. The data may be permanently transferred from the department to the Hennepin county medical center, and once transferred, shall continue to be classified as private data on individuals.

Subd. 3. Office of Health Facility Complaints; investigative data. Except for investigative data under section 626.556, all investigative data maintained by the Department of Health's Office of Health Facility Complaints are subject to provisions of and classified pursuant to section 626.557, subdivision 12b, paragraphs (b) to (d). Notwithstanding sections 626.556, subdivision 11, and 626.557, subdivision 12b, paragraph (b), data identifying an individual substantiated as the perpetrator are public data. For purposes of this subdivision, an individual is substantiated as the perpetrator if the commissioner of health determines that the individual is the perpetrator and the determination of the commissioner is upheld after the individual either exercises applicable administrative appeal rights or fails to exercise these rights within the time allowed by law.

13.3806. Public health data coded elsewhere

Subdivision 1. Scope. The sections referred to in subdivisions 2 to 20 are codified outside this chapter. Those sections classify data on public health as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 1a. Death investigation data. Data gathered by the commissioner of health to identify the body of a person believed to have died due to a declared emergency as defined in section 12.03, subdivision 1e, the circumstances of death, and disposition of the body are classified in and may be released according to section 12.381, subdivision 2.

Subd. 2. Certain epidemiologic studies. Use of data collected by the commissioner of health under sections 176.234, 268.19, and 270B.14, subdivision 11, is governed by section 144.0525.

Subd. 3. Public health studies. Data held by the commissioner of health in connection with public health studies are classified under section 144.053.

Subd. 4. Vital statistics.

(a) Parents' social security number; birth record. Parents' social security numbers provided for a child's birth record are classified under section 144.215, subdivision 4.

(b) Foundling registration. The report of the finding of an infant of unknown parentage is classified under section 144.216, subdivision 2.

(c) New record of birth. In circumstances in which a new record of birth may be issued under section 144.218, the original record of birth is classified as provided in that section.

(d) Vital records. Physical access to vital records is governed by section 144.225, subdivision 1.

(e) Birth record of child of unmarried parents. Access to the birth record of a child whose parents were not married to each other when the child was conceived or born is governed by sections 144.225, subdivisions 2 and 4, and 257.73.

(f) Health data for birth registration. Health data collected for birth registration or fetal death reporting are classified under section 144.225, subdivision 2a.

(g) Birth record; sharing. Sharing of birth record data and data prepared under section 257.75, is governed by section 144.225, subdivision 2b.

(h) Group purchaser identity for birth registration. Classification of and access to the identity of a group purchaser collected in association with birth registration is governed by section 144.225, subdivision 6.

Subd. 4a. Birth defects information system. Information collected for the birth defects information system is governed by section 144.2217.

Subd. 5. School health records.

(a) Student health data. Data collected for the health record of a school child are governed by section 144.29.

(b) Tuberculosis screening. Access to health records of persons enrolled in or employed by a school or school district for tuberculosis screening purposes is governed by section 144.441, subdivision 8.

Subd. 6. Health records. Access to health records is governed by section 144.335.

Subd. 7. Immunization data. Sharing of immunization data is governed by section 144.3351.

Subd. 8. Hepatitis B maternal carrier. Sharing of information regarding the hepatitis B infection status of a newborn's mother is governed by section 144.3352.

Subd. 9. Human leukocyte antigen type registry. Data identifying a person and the person's human leukocyte antigen type which is maintained by a government entity are classified under section 144.336, subdivision 1.

Subd. 10. Health threat procedures. Data in a health directive issued by the commissioner of health or a board of health are classified in section 144.4186.

Subd. 10a. Isolation or quarantine directive. Data in a directive issued by the commissioner of health under section 144.4195, subdivision 2, to isolate or quarantine a person or group of persons are classified in section 144.4195, subdivision 6.

Subd. 11. Tuberculosis health threat. Data collected by the commissioner of health in connection with a tuberculosis health threat are classified under

section 144.4813.

Subd. 12. Epidemiologic data. Epidemiologic data that identify individuals are classified under section 144.6581.

Subd. 13. Traumatic injury. Data on individuals with a brain or spinal injury collected by the commissioner of health are classified under section 144.665.

Subd. 14. Cancer surveillance system. Data on individuals collected by the cancer surveillance system are classified pursuant to section 144.69.

Subd. 15. Bloodborne pathogens. Data sharing between the emergency medical services agency and facilities is governed by section 144.7402, subdivision 3.

Subd. 16. Test information. Information concerning test results is governed by section 144.7411.

Subd. 17. Lead exposure. Data on individuals exposed to lead in their residences are classified under sections 144.9502, subdivision 9, and 144.9504, subdivision 2.

Subd. 18. Terminated pregnancies. Disclosure of reports of terminated pregnancies made to the commissioner of health is governed by section 145.413, subdivision 1.

Subd. 19. Repealed by Laws 2001, c. 211, § 4.

Subd. 19a. Maternal death. Access to and classification of medical data and health records related to maternal death studies are governed by section 145.901.

Subd. 20. Hazardous substance exposure. Disclosure of data related to hazardous substance exposure is governed by section 145.94.

13.381. Health regulatory data coded elsewhere

Subdivision 1. Scope. The sections referred to in subdivisions 2 to 17 are codified outside this chapter. Those sections classify health regulatory data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. Health occupations data.

(a) Health-related licensees and registrants. The collection, analysis, reporting, and use of data on individuals licensed or registered by the commissioner of health or health-related licensing boards are governed by sections 144.051, subdivision 2, and 144.052.

(b) Health services personnel. Data collected by the commissioner of health for the database on health services personnel are classified under section 144.1485.

Subd. 3. Nursing home residents. Access to certain data on assessments of care and services to nursing home residents is governed by section 144.0721, subdivision 2.

Subd. 4. Rural hospital grants. Financial data on individual hospitals under the rural hospital grant program are classified under section 144.147, subdivision 5.

Subd. 5. Certain health inspections. Disclosure of certain data received by the commissioner of health under sections 144.50 to 144.56 is governed by section 144.58.

Subd. 6. Public hospital meetings. Data from a closed meeting of a public hospital are classified under section 144.581, subdivision 5.

Subd. 7. Medical malpractice claims reports. Reports of medical malpractice claims submitted by an insurer to the commissioner of health under section 144.693 are classified as provided in section 144.693, subdivisions 1 and 2.

Subd. 7a. Facility requirements. Data provided to, filed with, or created or obtained by the commissioner of health under section 144.7065 are classified as provided in section 144.7065, subdivision 10.

Subd. 8. Health test results. Health test results obtained under sections 144.7401 to 144.7415 are classified under section 144.7411.

Subd. 9. Nursing home noncompliance. Data from correction orders of or notices of noncompliance by nursing homes are governed under section 144A.10.

Subd. 10. Home care and hospice provider. Data regarding a home care provider under sections 144A.43 to 144A.47 are governed by section 144A.45. Data regarding a hospice provider under sections 144A.75 to 144A.755 are governed by sections 144A.752 and 144A.754.

Subd. 11. Health facility complaints. Information gathered by the director of the office of health facility complaints is classified under section 144A.53, subdivision 3.

Subd. 12. Ambulance service data. Data required to be reported by ambulance services under section 144E.123 are classified under that section.

Subd. 13. Review organization data. Disclosure of data and information acquired by a review organization as defined in section 145.61, subdivision 5, is governed by section 145.64.

Subd. 14. Family planning grants. Information gathered under section 145.925 is classified under section 145.925, subdivision 6.

Subd. 15. Mortuary science interns. Data collected in case reports filed with the commissioner of health by mortuary science interns are classified under section 149A.20, subdivision 6.

Subd. 16. Funeral establishments. Data on individuals in annual reports required of certain funeral establishments are classified under section 149A.97, subdivision 11.

Subd. 17. Technology assistance review panel. Data maintained by the technology assistance review panel under section 256.9691, subdivision 6, are classified under that section.

13.383. Health occupations investigative data coded elsewhere

Subdivision 1. Scope. The sections referred to in subdivisions 2 to 16 are codified outside this chapter. Those sections classify health occupations investigative data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. EMT, EMT-I, EMT-P, or first responders. Reports of emergency medical technician, emergency medical technician-intermediate, emergency medical technician-paramedic, or first responder misconduct are classified under section 144E.305, subdivision 3.

Subd. 3. Unlicensed practitioners. Data relating to investigations and disciplinary actions under section 146A.06 are governed by subdivision 2 of that section.

Subd. 4. Physicians.

(a) Disciplinary data generally. Data held by the board of medical practice in connection with disciplinary matters are classified under section 147.01, subdivision 4. The administrative record of any disciplinary action taken by the board of medical practice under sections 147.01 to 147.22 is sealed upon judicial review as provided in section 147.151.

(b) Required examinations; physician's medical record. Data obtained by the board of medical practice when requiring a mental or physical examination of a physician or when accessing a physician's medical records are classified under section 147.091, subdivision 6.

(c) Sexual misconduct. Certain data relating to sexual misconduct are classified under section 147.092.

(d) Reports of violations. Certain reports of violations submitted to the board of medical practice are classified under section 147.121.

(e) Patient medical records. Patient medical records provided to the board of medical practice under section 147.131 are classified under that section.

Subd. 5. Physician assistants.

(a) Required examinations; physician assistant's medical records. Data obtained by the medical practices board when requiring a mental or physical examination of a physician assistant or when accessing a physician assistant's medical records are classified under section 147A.13, subdivision 6.

(b) Sharing complaint information. Sharing of complaint information regarding a physician assistant is governed by section 147A.26.

Subd. 6. Chiropractors. Data of the board of chiropractic examiners and the peer review committee are classified under sections 148.10, subdivision 1, and 148.106, subdivision 10.

Subd. 7. Nurses.

(a) Required examinations; nurse's medical records. Data obtained by the board of nursing when requiring a mental or physical examination of a nurse or when accessing a nurse's medical records are classified under section 148.261, subdivision 5.

(b) Reports of violations. Certain reports of violations submitted to the board of nursing are classified under section 148.264.

(c) Patient medical records. Medical records of a patient cared for by a nurse who is under review by the board of nursing are classified under sections 148.191, subdivision 2, and 148.265.

(d) Records of nurse disciplinary action. The administrative records of any disciplinary action taken by the board of nursing under sections 148.171 to 148.285 are sealed upon judicial review as provided in section 148.266.

Subd. 8. Psychologists and psychological practitioners. Client records of a patient cared for by a psychologist or psychological practitioner who is under review by the board of psychology are classified under section 148.941, subdivision 4. Data obtained by the board of psychology when requiring a mental, physical, or chemical dependency examination or evaluation of a regulated individual or when accessing the medical records of a regulated individual are classified under section 148.941, subdivision 8.

Subd. 9. Marriage and family therapists.

(a) Disciplinary data generally. Data held by the board of marriage and family therapy in connection with disciplinary matters are classified under sections 148B.04 and 148B.175, subdivisions 2 and 5.

(b) Reports of violations. Certain reports of violations submitted to the board of marriage and family therapy are classified under section 148B.08.

(c) Client records. Client records of a patient cared for by a marriage and family therapist who is under review by the board of marriage and family therapy are classified under sections 148B.09 and 148B.11.

Subd. 10. Social workers.

(a) Disciplinary data generally. Data held by the Board of Social Work in connection with disciplinary matters are classified under sections 148D.255 to 148D.270.

(b) Reports of violations. Certain reports of violations submitted to the Board of Social Work are classified under sections 148D.240 to 148D.250.

(c) Client records. Client records of a patient cared for by a social worker who is under review by the Board of Social Work are classified under section 148D.230.

Subd. 11. Unlicensed mental health practitioner.

(a) Disciplinary data generally. Data held by the commissioner of health in connection with the investigation of an unlicensed mental health practitioner are classified under section 148B.66, subdivision 2. The administrative records of disciplinary action taken by the commissioner of health pursuant to sections 148B.60 to 148B.71 are sealed upon judicial review as provided in section 148B.65.

(b) Client records. Client records of a patient cared for by an unlicensed mental health practitioner who is under review by the commissioner of health are classified under section 148B.66, subdivision 1.

(c) Required examinations; practitioner's medical records. Data obtained by the commissioner of health when requiring a mental or physical examination of an unlicensed mental health practitioner or when accessing the practitioner's medical records are classified under section 148B.68, subdivision 3.

Subd. 11a. Alcohol and drug counselor licensing; sharing. Sharing of data collected for licensing of alcohol and drug counselors is governed by section 148C.099, subdivision 2.

Subd. 12. Mortuary science practitioners. Data on investigations and disciplinary actions of mortuary science practitioners by the commissioner of health are classified under section 149A.04, subdivision 5.

Subd. 13. Dentists, dental hygienists, and dental assistants.

(a) Required examinations; medical records. Data obtained by the board of dentistry when requiring a mental or physical examination of a dentist, dental hygienist, or dental assistant or when accessing the medical records of a dentist, dental hygienist, or dental assistant are classified under sections 150A.08, subdivisions 5 and 6, and 150A.081.

(b) Patient records. Patient records of a patient cared for by a dentist, dental hygienist, or dental assistant who is under review by the board of dentistry are classified under section 150A.081.

(c) Investigative data. Reports submitted to the board of dentistry containing information about violations are classified under section 150A.14.

Subd. 14. Doctors of podiatric medicine.

(a) Patient records. Patient records of a patient cared for by a doctor of podiatric medicine who is under review by the board of podiatric medicine are classified under section 153.20.

(b) Access to doctor's medical data. Access to the medical data of a doctor of podiatric medicine who is under review by the board of podiatric medicine is governed by section 153.21, subdivision 2.

Subd. 15. Hearing instrument dispensers.

(a) Sharing complaint information. Sharing of complaint information regarding a hearing instrument dispenser is governed by section 153A.15, subdivision 3.

(b) Medical records. Medical records obtained by the commissioner of health in the course of reviewing a hearing instrument dispenser are classified under section 153A.15, subdivision 3a.

Subd. 16. Veterinarians.

(a) client records. Veterinary records on clients of a veterinarian who is under review by the board of veterinary medicine are classified under section 156.082.

(b) Required examinations; veterinarian's medical record. Data obtained by the board of veterinary medicine when requiring a mental or physical examination of a veterinarian or when accessing the veterinarian's medical records are classified under section 156.125.

13.384. Medical data

Subdivision 1. Definition. As used in this section:

(a) "Directory information" means name of the patient, date admitted, and general condition.

(b) "Medical data" means data collected because an individual was or is a patient or client of a hospital, nursing home, medical center, clinic, health or nursing agency operated by a state agency or political subdivision including business and financial records, data provided by private health care facilities, and data provided by or about relatives of the individual.

Subd. 2. Public hospitals; directory information.

(a) During the time that a person is a patient in a hospital operated by a state agency or political subdivision under legal commitment, directory information is public data. After the person is released by termination of the person's legal commitment, the directory information is private data on individuals.

(b) If a person is a patient other than pursuant to commitment in a hospital controlled by a state agency or political subdivision, directory information is public data unless the patient requests otherwise, in which case it is private data on individuals.

(c) Directory information about an emergency patient who is unable to communicate which is public under this subdivision shall not be released until a reasonable effort is made to notify the next of kin. Although an individual has requested that directory information be private, the hospital may release directory information to a law enforcement agency pursuant to a lawful investigation pertaining to that individual.

Subd. 3. Classification of medical data. Unless the data is summary data or a statute specifically provides a different classification, medical data are private but are available only to the subject of the data as provided in section 144.335, and shall not be disclosed to others except:

(a) Pursuant to section 13.05;

(b) Pursuant to section 253B.0921;

(c) Pursuant to a valid court order;

(d) To administer federal funds or programs;

(e) To the surviving spouse, parents, children, and siblings of a deceased patient or client or, if there are no surviving spouse, parents, children, or siblings, to the surviving heirs of the nearest degree of kindred;

(f) To communicate a patient's or client's condition to a family member or other appropriate person in accordance with acceptable medical practice, unless the patient or client directs otherwise; or

(g) As otherwise required by law.

13.385. Renumbered 13.3805, subd. 2, in St.2000

Attorney, Audit, and Investigative Data

13.39. Civil investigation

Subdivision 1. Definitions. A "pending civil legal action" includes but is not limited to judicial, administrative or arbitration proceedings. Whether a civil legal action is pending shall be determined by the chief attorney acting for the state agency, political subdivision or statewide system.

Subd. 2. Civil actions.

(a) Except as provided in paragraph (b), data collected by state agencies, political subdivisions, or statewide systems as part of an active investigation undertaken for the purpose of the commencement or defense of a pending civil legal action, or which are retained in anticipation of a pending civil legal action, are classified as protected nonpublic data pursuant to section 13.02, subdivision 13, in the case of data not on individuals and confidential pursuant to section 13.02, subdivision 3, in the case of data on individuals. Any agency, political subdivision, or statewide system may make any data classified as confidential or protected nonpublic pursuant to this subdivision accessible to any person, agency or the public if the agency, political subdivision, or statewide system determines that the access will aid the law enforcement process, promote public health or safety or dispel widespread rumor or unrest.

(b) A complainant has access to a statement provided by the complainant to a state agency, statewide system, or political subdivision under paragraph (a).

Subd. 2a. Disclosure of data. During the time when a civil legal action is determined to be pending under subdivision 1, any person may bring an action in the district court in the county where the data is maintained to obtain disclosure of data classified as confidential or protected nonpublic under subdivision 2. The court may order that all or part of the data be released to the public or to the person bringing the action. In making the determination whether data shall be disclosed, the court shall consider whether the benefit to the person bringing the action or to the public outweighs any harm to the public, the agency, or any person identified in the data. The data in dispute shall be examined by the court in camera.

Subd. 3. Inactive investigative data. Inactive civil investigative data are public, unless the release of the data would jeopardize another pending civil legal action, and except for those portions of a civil investigative file that are classified as not public data by this chapter or other law. Any civil investigative data presented as evidence in court or made part of a court record shall be public. Civil investigative data become inactive upon the occurrence of any of the following events:

(1) a decision by the state agency, political subdivision, or statewide system or by the chief attorney acting for the state agency, political subdivision, or statewide system not to pursue the civil action;

(2) expiration of the time to file a complaint under the statute of limitations or agreement applicable to the civil action; or

(3) exhaustion of or expiration of rights of appeal by either party to the civil action.

Data determined to be inactive under clause (1) may become active if the state agency, political subdivision, statewide system, or its attorney decides to renew the civil action.

13.391. Renumbered 13.821 in St.2000

13.392. Internal auditing data

Subdivision 1. Confidential data or protected nonpublic data. Data, notes, and preliminary drafts of reports created, collected, and maintained by the internal audit offices of state agencies and political subdivisions, or persons performing audits for state agencies and political subdivisions, and relating to an audit or investigation are confidential data on individuals or protected nonpublic data until the final report has been published or the audit or investigation is no longer being pursued actively, except that the data shall be disclosed as required to comply with section 6.67 or 609.456. This section does not limit in any way:

(1) the state auditor's access to government data of political subdivisions or data, notes, or preliminary drafts of reports of persons performing audits for political subdivisions; or

(2) the public or a data subject's access to data classified by section 13.43.

Subd. 2. Private data on individuals. Data on an individual supplying information for an audit or investigation, that could reasonably be used to determine the individual's identity, are private data on individuals if the information supplied was needed for an audit or investigation and would not have been provided to the internal audit office or person performing audits without an assurance to the individual that the individual's identity would remain private.

13.393. Attorneys

Notwithstanding the provisions of this chapter and section 15.17, the use, collection, storage, and dissemination of data by an attorney acting in a professional capacity for the state, a state agency or a political subdivision shall be governed by statutes, rules, and professional standards concerning discovery, production of documents, introduction of evidence, and professional responsibility; provided that this section shall not be construed to affect the applicability of any statute, other than this chapter and section 15.17, which specifically requires or prohibits disclosure of specific information by the attorney, nor shall this section be construed to relieve any responsible authority, other than the attorney, from duties and responsibilities pursuant to this chapter and section 15.17.

Library Data

13.40. Library and historical data

Subdivision 1. Records subject to this chapter.

(a) For purposes of this section, "historical records repository" means an archives or manuscript repository operated by any state agency, statewide system, or political subdivision whose purpose is to collect and maintain data to further the history of a geographic or subject area. The term does not include the state archives as defined in section 138.17, subdivision 1, clause (5).

(b) Data collected, maintained, used, or disseminated by a library or historical records repository operated by any state agency, political subdivision, or statewide system shall be administered in accordance with the provisions of this chapter.

Subd. 2. Private data; library borrowers.

(a) Except as provided in paragraph (b), the following data maintained by a library are private data on individuals and may not be disclosed for other than library purposes except pursuant to a court order:

(1) data that link a library patron's name with materials requested or borrowed by the patron or that link a patron's name with a specific subject about which the patron has requested information or materials; or

(2) data in applications for borrower cards, other than the name of the borrower.

(b) A library may release reserved materials to a family member or other person who resides with a library patron and who is picking up the material on behalf of the patron. A patron may request that reserved materials be released only to the patron.

Subd. 3. Nongovernmental data. Data held in the custody of a historical records repository that were not originally created, received, maintained, or disseminated by a state agency, statewide system, or political subdivision are not government data. These data are accessible to the public unless:

(1) the data are contributed by private persons under an agreement that restricts access, to the extent of any lawful limitation; or

(2) access would significantly endanger the physical or organizational integrity of the data.

13.401. Library and historical data coded elsewhere

Subdivision 1. Scope. The section referred to in subdivision 2 is codified outside this chapter. That section places a restriction on access to government data.

Subd. 2. Restrictions on access to archives records. Limitations on access to records transferred to the state archives are provided in section 138.17, subdivision 1c.

Licensing Data

13.41. Licensing data

Subdivision 1. Definition. As used in this section "licensing agency" means any board, department or agency of this state which is given the statutory authority to issue professional or other types of licenses, except the various agencies primarily administered by the commissioner of human services. Data pertaining to persons or agencies licensed or registered under authority of the commissioner of human services shall be administered pursuant to section 13.46.

Subd. 2. Private data; designated addresses and telephone numbers.

(a) The following data collected, created or maintained by any licensing agency are classified as private, pursuant to section 13.02, subdivision 12: data, other than their names and designated addresses, submitted by applicants for licenses; the identity of complainants who have made reports concerning licensees or applicants which appear in inactive complaint data unless the complainant consents to the disclosure; the nature or content of unsubstantiated complaints when the information is not maintained in anticipation of legal action; the identity of patients whose medical records are received by any health licensing agency for purposes of review or in anticipation of a contested matter; inactive investigative data relating to violations of statutes or rules; and the record of any disciplinary proceeding except as limited by subdivision 5.

(b) An applicant for a license shall designate on the application a residence or business address and telephone number at which the applicant can be contacted in connection with the license application. A licensee shall designate a residence or business address and telephone number at which the licensee can be contacted in connection with the license. By designating an address under this paragraph other than a residence address, the applicant or licensee consents to accept personal service of process by service on the licensing agency for legal or administrative proceedings. The licensing agency shall mail a copy of the documents to the applicant or licensee at the last known residence address.

Subd. 3. Board of peace officer standards and training. The following government data of the board of peace officer standards and training are private data:

(1) home addresses of licensees and applicants for licenses; and

(2) data that identify the state agency, statewide system, or political subdivision that employs a licensed peace officer.

The board may disseminate private data on applicants and licensees as is necessary to administer law enforcement licensure or to provide data under section 626.845, subdivision 1, to law enforcement agencies who are conducting employment background investigations.

Subd. 4. Confidential data. The following data collected, created or maintained by any licensing agency are classified as confidential, pursuant to section 13.02, subdivision 3: active investigative data relating to the investigation of complaints against any licensee.

Subd. 5. Public data. Licensing agency minutes, application data on licensees except nondesignated addresses, orders for hearing, findings of fact, conclusions of law and specification of the final disciplinary action contained in the record of the disciplinary action are classified as public, pursuant to section 13.02, subdivision 15. The entire record concerning the disciplinary proceeding is public data pursuant to section 13.02, subdivision 15, in those instances where there is a public hearing concerning the disciplinary action. If the licensee and the licensing agency agree to resolve a complaint without a hearing, the agreement and the specific reasons for the agreement are public data. The license numbers, the license status, and continuing education records issued or maintained by the board of peace officer standards and training are classified as public data, pursuant to section 13.02, subdivision 15.

Subd. 6. Releasing data. Any licensing agency may make any data classified as private or confidential pursuant to this section accessible to an appropriate person or agency if the licensing agency determines that failure to make the data accessible is likely to create a clear and present danger to public health or safety.

13.411. Licensing data coded elsewhere

Subdivision 1. Scope. The sections referred to in subdivisions 2 to 8 are codified outside this chapter. Those sections classify licensing data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. Home care providers. Data from criminal background studies of the owner or managerial official of a home care provider that are given to the commissioner of health are classified under section 144A.46, subdivision 5.

Subd. 3. Unlicensed complementary and alternative health care practitioners and clients. Data obtained by the commissioner of health on unlicensed complementary and alternative health care practitioners and clients are classified under sections 146A.06 and 146A.08.

Subd. 4. Marriage and family therapists. Residence addresses and telephone numbers of marriage and family therapist licensees are classified under section 148B.04, subdivision 6.

Subd. 5. Social workers. Residence addresses and telephone numbers of social worker licensees are classified under chapter 148D.

Subd. 6. Practitioners of mortuary science.

(a) Mortuary science. Data submitted to the commissioner of health for a license, reciprocal license, or renewal of a license to practice mortuary science are classified under sections 149A.20, subdivision 13, 149A.30, subdivision 7, and 149A.40, subdivision 10.

(b) Operation of funeral establishment. Data submitted to the commissioner of health for a license or renewal of a license to operate a funeral establishment are classified under sections 149A.50, subdivision 9, and 149A.51, subdivision 9.

(c) Operation of a crematory. Data submitted to the commissioner of health for a license or renewal of a license to operate a crematory are classified under sections 149A.52, subdivision 8, and 149A.53, subdivision 8.

Subd. 7. Examining and licensing boards.

(a) Health licensing boards. Data held by health licensing boards are classified under sections 214.10, subdivision 8, and 214.25, subdivision 1.

(b) Combined boards data. Data held by licensing boards participating in a health professional services program are classified under sections 214.34 and 214.35.

Subd. 8. Private detective license. Certain data on applicants for licensure as private detectives are classified under section 326.3382, subdivision 3.

13.42. Renumbered 13.384 in St.2000

Personnel; Salary Benefit Data

13.43. Personnel data

Subdivision 1. Definition. As used in this section, "personnel data" means data on individuals collected because the individual is or was an employee of or an applicant for employment by, performs services on a voluntary basis for, or acts as an independent contractor with a government entity. Personnel data includes data submitted by an employee to a government entity as part of an organized self-evaluation effort by the government entity to request suggestions from all employees on ways to cut costs, make government more efficient, or improve the operation of government. An employee who is identified in a suggestion shall have access to all data in the suggestion except the identity of the employee making the suggestion.

Subd. 2. Public data.

(a) Except for employees described in subdivision 5 and subject to the limitations described in subdivision 5a, the following personnel data on current and former employees, volunteers, and independent contractors of a government entity is public:

(1) name; employee identification number, which must not be the em-

ployee's Social Security number; actual gross salary; salary range; contract fees; actual gross pension; the value and nature of employer paid fringe benefits; and the basis for and the amount of any added remuneration, including expense reimbursement, in addition to salary;

(2) job title and bargaining unit; job description; education and training background; and previous work experience;

(3) date of first and last employment;

(4) the existence and status of any complaints or charges against the employee, regardless of whether the complaint or charge resulted in a disciplinary action;

(5) the final disposition of any disciplinary action together with the specific reasons for the action and data documenting the basis of the action, excluding data that would identify confidential sources who are employees of the public body;

(6) the terms of any agreement settling any dispute arising out of an employment relationship, including a buyout agreement as defined in section 123B.143, subdivision 2, paragraph (a); except that the agreement must include specific reasons for the agreement if it involves the payment of more than $10,000 of public money;

(7) work location; a work telephone number; badge number; and honors and awards received; and

(8) payroll time sheets or other comparable data that are only used to account for employee's work time for payroll purposes, except to the extent that release of time sheet data would reveal the employee's reasons for the use of sick or other medical leave or other not public data.

(b) For purposes of this subdivision, a final disposition occurs when the state agency, statewide system, or political subdivision makes its final decision about the disciplinary action, regardless of the possibility of any later proceedings or court proceedings. In the case of arbitration proceedings arising under collective bargaining agreements, a final disposition occurs at the conclusion of the arbitration proceedings, or upon the failure of the employee to elect arbitration within the time provided by the collective bargaining agreement. Final disposition includes a resignation by an individual when the resignation occurs after the final decision of the state agency, statewide system, political subdivision, or arbitrator.

(c) The state agency, statewide system, or political subdivision may display a photograph of a current or former employee to a prospective witness as part of the state agency's, statewide system's, or political subdivision's investigation of any complaint or charge against the employee.

(d) A complainant has access to a statement provided by the complainant to a state agency, statewide system, or political subdivision in connection with a complaint or charge against an employee.

(e) Notwithstanding paragraph (a), clause (5), upon completion of an investigation of a complaint or charge against a public official, or if a public official resigns or is terminated from employment while the complaint or charge is pending, all data relating to the complaint or charge are public, unless access to the data would jeopardize an active investigation or reveal confidential sources. For purposes of this paragraph, "public official" means:

(1) the head of a state agency and deputy and assistant state agency heads;

(2) members of boards or commissions required by law to be appointed by the governor or other elective officers; and

(3) executive or administrative heads of departments, bureaus, divisions, or institutions.

Subd. 2a. Data disclosure by statewide pension plans. Notwithstanding any law to the contrary, with respect to data collected and maintained on members, survivors, and beneficiaries by statewide retirement systems that is classified as public data in accordance with subdivision 2, those retirement systems may be only required to disclose name, gross pension, and type of benefit awarded, except as required by sections 13.03, subdivisions 4 and 6; and 13.05, subdivisions 4 and 9.

Subd. 3. Applicant data. Except for applicants described in subdivision 5, the following personnel data on current and former applicants for employment by a government entity is public: veteran status; relevant test scores; rank on eligible list; job history; education and training; and work availability. Names of applicants shall be private data except when certified as eligible for appointment to a vacancy or when applicants are considered by the appointing authority to be finalists for a position in public employment. For purposes of this subdivision, "finalist" means an individual who is selected to be interviewed by the appointing authority prior to selection.

Subd. 4. Other data. All other personnel data is private data on individuals but may be released pursuant to a court order. Data pertaining to an employee's dependents are private data on individuals.

Subd. 5. Undercover law enforcement officer. All personnel data maintained by any state agency, statewide system or political subdivision relating to an individual employed as or an applicant for employment as an undercover law enforcement officer are private data on individuals. When the individual is no longer assigned to an undercover position, the data described in subdivisions 2 and 3 become public unless the law enforcement agency determines that revealing the data would threaten the personal safety of the officer or jeopardize an active investigation.

Subd. 5a. Limitation on disclosure of certain personnel data. Notwithstanding any other provision of this section, the following data relating to employees of a secure treatment facility defined in section 253B.02, subdivision 18a, employees of a state correctional facility, or employees of the Department of Corrections directly involved in supervision of offenders in the community, shall not be disclosed to facility patients, corrections inmates, or other individuals who facility or correction administrators reasonably believe will use the information to harass, intimidate, or assault any of these employees: place where previous education or training occurred; place of prior employment; and payroll timesheets or other comparable data, to the extent that disclosure of payroll timesheets or other comparable data may disclose future work assignments, home address or telephone number, the location of an employee during nonwork hours, or the location of an employee's immediate family members.

Subd. 6. Access by labor organizations. Personnel data may be disseminated to labor organizations to the extent that the responsible authority determines that the dissemination is necessary to conduct elections, notify employees of fair share fee assessments, and implement the provisions of chapters 179 and 179A. Personnel data shall be disseminated to labor organizations and to the bureau of mediation services to the extent the dissemination is ordered or authorized by the commissioner of the bureau of mediation services.

Subd. 7. Employee assistance data. All data created, collected or maintained by any state agency or political subdivision to administer employee assistance programs similar to the one authorized by section 43A.319 are classified as private, pursuant to section 13.02, subdivision 12. This section shall not be interpreted to authorize the establishment of employee assistance programs.

Subd. 8. Harassment data. When allegations of sexual or other types of harassment are made against an employee, the employee does not have access to data that would identify the complainant or other witnesses if the responsible authority determines that the employee's access to that data would:

(1) threaten the personal safety of the complainant or a witness; or

(2) subject the complainant or witness to harassment.

If a disciplinary proceeding is initiated against the employee, data on the complainant or witness shall be available to the employee as may be necessary for the employee to prepare for the proceeding.

Subd. 9. Peer counseling debriefing data.

(a) Data acquired by a peer group member in a public safety peer counseling debriefing is private data on the person being debriefed.

(b) For purposes of this subdivision, "public safety peer counseling debriefing" means a group process oriented debriefing session held for peace officers, firefighters, medical emergency persons, dispatchers, or other persons involved with public safety emergency services, that is established by any agency providing public safety emergency services and is designed to help a person who has suffered an occupation-related traumatic event begin the process of healing and effectively dealing with posttraumatic stress.

Subd. 10. Prohibition on agreements limiting disclosure or discussion of personnel data.

(a) A state agency, statewide system, or political subdivision may not enter into an agreement settling a dispute arising out of the employment relationship with the purpose or effect of limiting access to or disclosure of personnel data or limiting the discussion of information or opinions related to personnel data. An agreement or portion of an agreement that violates this paragraph is void and unenforceable.

(b) Paragraph (a) applies to the following, but only to the extent that the data or information could otherwise be made accessible to the public:

(1) an agreement not to discuss, publicize, or comment on personnel data or information;

(2) an agreement that limits the ability of the subject of personnel data to release or consent to the release of data; or

(3) any other provision of an agreement that has the effect of limiting the disclosure or discussion of information that could otherwise be made accessible to the public, except a provision that limits the ability of an employee to release or discuss private data that identifies other employees.

(c) Paragraph (a) also applies to a court order that contains terms or conditions prohibited by paragraph (a).

Subd. 11. Protection of employee or others.

(a) If the responsible authority or designee of a state agency, statewide system, or political subdivision reasonably determines that the release of personnel data is necessary to protect an employee from harm to self or to protect another person who may be be released as provided in this subdivision.

(b) The data may be released:

(1) to the person who may be harmed and to an attorney representing the person when the data are relevant to obtaining a restraining order;

(2) to a prepetition screening team conducting an investigation of the employee under section 253B.07, subdivision 1; or

(3) to a court, law enforcement agency, or prosecuting authority.

(c) Section 13.03, subdivision 4, paragraph (c), applies to data released under this subdivision, except to the extent that the data have a more restrictive classification in the possession of the agency or authority that receives the data. If the person who may be harmed or the person's attorney receives data under this subdivision, the data may be used or released further only to the extent necessary to protect the person from harm.

Subd. 12. Sharing of law enforcement personnel background investigation data. A law enforcement agency shall share data from a background investigation done under section 626.87 with the peace officer standards and training board or with a law enforcement agency doing an investigation of the subject of the data under section 626.87.

Subd. 13. Dissemination of data to Department of Employment and Economic Development. Private personnel data must be disclosed to the department of employment and economic development for the purpose of administration of the unemployment benefits program under chapter 268.

Subd. 14. Maltreatment data. When a report of alleged maltreatment of a student in a school facility, as defined in section 626.556, subdivision 2, paragraph (f), is made to the commissioner of education under section 626.556, data that are relevant to a report of maltreatment and are collected by the school facility about the person alleged to have committed maltreatment must be provided to the commissioner of education upon request for purposes of an assessment or investigation of the maltreatment report. Data received by the commissioner of education pursuant to these assessments or investigations are classified under section 626.556.

Subd. 15. Dissemination of data to law enforcement. Private personnel data, or data on employees that are confidential data under section 13.39, may be disseminated to a law enforcement agency for the purpose of reporting a crime or alleged crime committed by an employee, or for the purpose of assisting law enforcement in the investigation of a crime committed or allegedly committed by an employee.

Subd. 16. School district or charter school disclosure of violence or inappropriate sexual contact. The superintendent of a school district or the superintendent's designee, or a person having administrative control of a charter school, must release to a requesting school district or charter school private personnel data on a current or former employee related to acts of violence toward or sexual contact with a student, if an investigation conducted by or on behalf of the school district or law enforcement affirmed the allegations in writing prior to release and the investigation resulted in the resignation of the subject of the data.

13.435. Salary benefit survey data

Salary and personnel benefit survey data purchased from consulting firms, nonprofit corporations or associations or obtained from employers with the written understanding that the data shall not be made public which is maintained by state agencies, political subdivisions or statewide systems are classified as nonpublic pursuant to section 13.02, subdivision 9.

Property Data

13.44. Property data

Subdivision 1. Real property; complaint data. The identities of individuals who register complaints with state agencies or political subdivisions concerning violations of state laws or local ordinances concerning the use of real property are classified as confidential data, pursuant to section 13.02, subdivision 3.

Subd. 2. Real property; building code violations. Code violation records pertaining to a particular parcel of real property and the buildings, improvements, and dwelling units located on it that are kept by any state, county, or city agency charged by the governing body of the appropriate political subdivision with the responsibility for enforcing a state, county, or city health, housing, building, fire prevention, or housing maintenance code are public data; except as otherwise provided by section 13.39, subdivision 2; 13.44; or 13.82, subdivision 7.

Subd. 3. Real property; appraisal data.

(a) Confidential or protected nonpublic data. Estimated or appraised values of individual parcels of real property that are made by personnel of the state or a political subdivision or by independent appraisers acting for the state or a political subdivision for the purpose of selling or acquiring land through purchase or condemnation are classified as confidential data on individuals or protected nonpublic data.

(b) Private or nonpublic data. Appraised values of individual parcels of real property that are made by appraisers working for fee owners or contract purchasers who have received an offer to purchase their property from the state or a political subdivision are classified as private data on individuals or nonpublic data.

(c) Public data. The data made confidential or protected nonpublic under paragraph (a) or made private or nonpublic under paragraph (b) become public upon the occurrence of any of the following:

(1) the data are submitted to a court-appointed condemnation commissioner;

(2) the data are presented in court in condemnation proceedings; or

(3) the negotiating parties enter into an agreement for the purchase and sale of the property.

Subd. 4. Personal and intangible property; appraisal data. Preliminary and final market value appraisals, which are made by personnel of a city or county or by an independent appraiser acting on behalf of a city or county, of personal and intangible property owned by the city or county, are classified as nonpublic data not on individuals until either (1) a purchase agreement is entered into; or (2) the parties negotiating the transaction exchange appraisals.

13.441. Property data coded elsewhere

Subdivision 1. Scope. The sections referred to in subdivisions 2 and 3 are codified outside this chapter. Those sections classify property data as other than public, place restrictions on access to government data, or involve data sharing.

Subd. 2. Trusts.

(a) Charitable trust data. Data filed by a charitable trust with the attorney general are governed by section 501B.39.

(b) Charitable trust data sharing. Data sharing of records of a charitable trust is governed by section 501B.40, subdivision 3.

Subd. 3. Probate; international will registration. Information on the execution of international wills is classified under section 524.2-1010,

Open Meetings

Minnesota Statutes Annotated

Meetings of Public Bodies (Ch. 13D)

Chapter 13D. Open Meeting Law

13D.01. Meetings must be open to the public; exceptions

Subdivision 1. In executive branch, local government. All meetings, including executive sessions, must be open to the public

(a) of a state

(1) agency,

(2) board,

(3) commission, or

(4) department,

when required or permitted by law to transact public business in a meeting;

(b) of the governing body of a

(1) school district however organized,

(2) unorganized territory,

(3) county,

(4) statutory or home rule charter city,

(5) town, or

(6) other public body;

(c) of any

(1) committee,

(2) subcommittee,

(3) board,

(4) department, or

(5) commission,

of a public body; and

(d) of the governing body or a committee of:

(1) a statewide public pension plan defined in section 356A.01, subdivision 24; or

(2) a local public pension plan governed by section 69.77, sections 69.771 to 69.775, or chapter 354A, 422A, or 423B.

Subd. 2. Exceptions. This chapter does not apply

(1) to meetings of the commissioner of corrections;

(2) to a state agency, board, or commission when it is exercising quasi-judicial functions involving disciplinary proceedings; or

(3) as otherwise expressly provided by statute.

Subd. 3. Subject of and grounds for closed meeting. Before closing a meeting, a public body shall state on the record the specific grounds permitting the meeting to be closed and describe the subject to be discussed.

(a) A meeting required by this section to be open to the public must be recorded in a journal kept for that purpose.

(b) The vote of each member must be recorded on each appropriation of money, except for payments of judgments, claims, and amounts fixed by statute.

Subd. 5. Public access to journal. The journal must be open to the public during all normal business hours where records of the public body are kept.

Subd. 6. Public copy of members' materials.

(a) In any meeting which under subdivisions 1, 2, 4, and 5, and section 13D.02 must be open to the public, at least one copy of any printed materials relating to the agenda items of the meeting prepared or distributed by or at the direction of the governing body or its employees and:

(1) distributed at the meeting to all members of the governing body;

(2) distributed before the meeting to all members; or

(3) available in the meeting room to all members;

shall be available in the meeting room for inspection by the public while the governing body considers their subject matter.

(b) This subdivision does not apply to materials classified by law as other than public as defined in chapter 13, or to materials relating to the agenda items of a closed meeting held in accordance with the procedures in section 13D.03 or other law permitting the closing of meetings.

13D.02. Meetings conducted by interactive TV; conditions

Subdivision 1. Conditions. A meeting governed by section 13D.01, subdivisions 1, 2, 4, and 5, and this section may be conducted by interactive television so long as:

(1) all members of the body participating in the meeting, wherever their physical location, can hear and see one another and can hear and see all discussion and testimony presented at any location at which at least one member is present;

(2) members of the public present at the regular meeting location of the body can hear and see all discussion and testimony and all votes of members of the body;

(3) at least one member of the body is physically present at the regular meeting location; and

(4) each location at which a member of the body is present is open and accessible to the public.

Subd. 2. Members are present for quorum, participation. Each member of a body participating in a meeting by electronic means is considered present at the meeting for purposes of determining a quorum and participating in all proceedings.

Subd. 3. Monitoring from remote site; costs. If interactive television is used to conduct a meeting, to the extent practical, a public body shall allow a person to monitor the meeting electronically from a remote location. The body may require the person making such a connection to pay for documented marginal costs that the public body incurs as a result of the additional connection.

Subd. 4. Notice of regular and all member sites. If interactive television is used to conduct a regular, special, or emergency meeting, the public body shall provide notice of the regular meeting location and notice of any site where a member of the public body will be participating in the meeting by interactive television. The timing and method of providing notice must be as described in section 13D.04.

13D.03. Closed meetings for labor negotiations strategy

Subdivision 1. Procedure.

(a) Section 13D.01, subdivisions 1, 2, 4, 5, and section 13D.02 do not apply to a meeting held pursuant to the procedure in this section.

(b) The governing body of a public employer may by a majority vote in a public meeting decide to hold a closed meeting to consider strategy for labor negotiations, including negotiation strategies or developments or discussion and review of labor negotiation proposals, conducted pursuant to sections 179A.01 to 179A.25.

(c) The time of commencement and place of the closed meeting shall be announced at the public meeting.

(d) A written roll of members and all other persons present at the closed meeting shall be made available to the public after the closed meeting.

Subd. 2. Meeting must be recorded.

(a) The proceedings of a closed meeting to discuss negotiation strategies shall be tape-recorded at the expense of the governing body.

(b) The recording shall be preserved for two years after the contract is signed and shall be made available to the public after all labor contracts are signed by the governing body for the current budget period.

Subd. 3. If violation claimed.

(a) If an action is brought claiming that public business other than discussions of labor negotiation strategies or developments or discussion and review of labor negotiation proposals was transacted at a closed meeting held pursuant to this section during the time when the tape is not available to the public, the court shall review the recording of the meeting in camera.

(b) If the court finds that this section was not violated, the action shall be dismissed and the recording shall be sealed and preserved in the records of the court until otherwise made available to the public pursuant to this section.

(c) If the court finds that this section was violated, the recording may be introduced at trial in its entirety subject to any protective orders as requested by either party and deemed appropriate by the court.

13D.04. Notice of meetings

Subdivision 1. Regular meetings. A schedule of the regular meetings of a public body shall be kept on file at its primary offices. If a public body decides to hold a regular meeting at a time or place different from the time or place stated in its schedule of regular meetings, it shall give the same notice of the meeting that is provided in this section for a special meeting.

Subd. 2. Special meetings.

(a) For a special meeting, except an emergency meeting or a special meeting for which a notice requirement is otherwise expressly established by statute, the public body shall post written notice of the date, time, place, and purpose of the meeting on the principal bulletin board of the public body, or if the public body has no principal bulletin board, on the door of its usual meeting room.

(b) The notice shall also be mailed or otherwise delivered to each person who has filed a written request for notice of special meetings with the public body. This notice shall be posted and mailed or delivered at least three days before the date of the meeting.

(c) As an alternative to mailing or otherwise delivering notice to persons who have filed a written request for notice of special meetings, the public body may publish the notice once, at least three days before the meeting, in the official newspaper of the public body or, if there is none, in a qualified newspaper of general circulation within the area of the public body's authority.

(d) A person filing a request for notice of special meetings may limit the request to notification of meetings concerning particular subjects, in which case the public body is required to send notice to that person only concerning special meetings involving those subjects.

(e) A public body may establish an expiration date for requests for notices of special meetings pursuant to this subdivision and require refiling of the request once each year.

(f) Not more than 60 days before the expiration date of a request for notice, the public body shall send notice of the refiling requirement to each person who filed during the preceding year.

Subd. 3. Emergency meetings.

(a) For an emergency meeting, the public body shall make good faith efforts to provide notice of the meeting to each news medium that has filed a written request for notice if the request includes the news medium's telephone number.

(b) Notice of the emergency meeting shall be given by telephone or by any other method used to notify the members of the public body.

(c) Notice shall be provided to each news medium which has filed a written request for notice as soon as reasonably practicable after notice has been given to the members.

(d) Notice shall include the subject of the meeting. Posted or published notice of an emergency meeting is not required.

(e) An "emergency" meeting is a special meeting called because of circumstances that, in the judgment of the public body, require immediate consideration by the public body.

(f) If matters not directly related to the emergency are discussed or acted upon at an emergency meeting, the minutes of the meeting shall include a specific description of the matters.

(g) The notice requirement of this subdivision supersedes any other statutory notice requirement for a special meeting that is an emergency meeting.

Subd. 4. Recessed or continued meetings.

(a) If a meeting is a recessed or continued session of a previous meeting, and the time and place of the meeting was established during the previous meeting and recorded in the minutes of that meeting, then no further published or mailed notice is necessary.

(b) For purposes of this subdivision, the term "meeting" includes a public hearing conducted pursuant to chapter 429 or any other law or charter provision requiring a public hearing by a public body.

Subd. 5. Closed meetings. The notice requirements of this section apply to closed meetings.

Subd. 6. State agencies. For a meeting of an agency, board, commission, or department of the state:

(1) the notice requirements of this section apply only if a statute governing meetings of the agency, board, or commission does not contain specific reference to the method of providing notice; and

(2) all provisions of this section relating to publication are satisfied by publication in the State Register.

Subd. 7. Actual notice. If a person receives actual notice of a meeting of a public body at least 24 hours before the meeting, all notice requirements of this section are satisfied with respect to that person, regardless of the method of receipt of notice.

13D.05. Meetings having data classified as not public

Subdivision 1. General principles.

(a) Except as provided in this chapter, meetings may not be closed to discuss data that are not public data.

(b) Data that are not public data may be discussed at a meeting subject to this chapter without liability or penalty, if the disclosure relates to a matter within the scope of the public body's authority and is reasonably necessary to conduct the business or agenda item before the public body.

(c) Data discussed at an open meeting retain the data's original classification; however, a record of the meeting, regardless of form, shall be public.

Subd. 2. When meeting must be closed.

(a) Any portion of a meeting must be closed if expressly required by other law or if the following types of data are discussed:

(1) data that would identify alleged victims or reporters of criminal sexual conduct, domestic abuse, or maltreatment of minors or vulnerable adults;

(2) active investigative data as defined in section 13.82, subdivision 7, or internal affairs data relating to allegations of law enforcement personnel misconduct collected or created by a state agency, statewide system, or political subdivision; or

(3) educational data, health data, medical data, welfare data, or mental health data that are not public data under section 13.32, 13.3805, subdivision 1, 13.384, or 13.46, subdivision 2 or 7.

(b) A public body shall close one or more meetings for preliminary consideration of allegations or charges against an individual subject to its authority. If the members conclude that discipline of any nature may be warranted as a result of those specific charges or allegations, further meetings or hearings relating to those specific charges or allegations held after that conclusion is reached must be open. A meeting must also be open at the request of the individual who is the subject of the meeting.

Subd. 3. What meetings may be closed.

(a) A public body may close a meeting to evaluate the performance of an individual who is subject to its authority. The public body shall identify the individual to be evaluated prior to closing a meeting. At its next open meet-

ing, the public body shall summarize its conclusions regarding the evaluation. A meeting must be open at the request of the individual who is the subject of the meeting.

(b) Meetings may be closed if the closure is expressly authorized by statute or permitted by the attorney-client privilege.

(c) A public body may close a meeting:

(1) to determine the asking price for real or personal property to be sold by the government entity;

(2) to review confidential or nonpublic appraisal data under section 13.44, subdivision 3; and

(3) to develop or consider offers or counteroffers for the purchase or sale of real or personal property.

Before holding a closed meeting under this paragraph, the public body must identify on the record the particular real or personal property that is the subject of the closed meeting. The proceedings of a meeting closed under this paragraph must be tape recorded at the expense of the public body. The recording must be preserved for eight years after the date of the meeting and made available to the public after all real or personal property discussed at the meeting has been purchased or sold or the governing body has abandoned the purchase or sale. The real or personal property that is the subject of the closed meeting must be specifically identified on the tape. A list of members and all other persons present at the closed meeting must be made available to the public after the closed meeting. If an action is brought claiming that public business other than discussions allowed under this paragraph was transacted at a closed meeting held under this paragraph during the time when the tape is not available to the public, section 13D.03, subdivision 3, applies.

An agreement reached that is based on an offer considered at a closed meeting is contingent on approval of the public body at an open meeting. The actual purchase or sale must be approved at an open meeting after the notice period required by statute or the governing body's internal procedures, and the purchase price or sale price is public data.

(d) Meetings may be closed to receive security briefings and reports, to discuss issues related to security systems, to discuss emergency response procedures and to discuss security deficiencies in or recommendations regarding public services, infrastructure and facilities, if disclosure of the information discussed would pose a danger to public safety or compromise security procedures or responses. Financial issues related to security matters must be discussed and all related financial decisions must be made at an open meeting. Before closing a meeting under this paragraph, the public body, in describing the subject to be discussed, must refer to the facilities, systems, procedures, services, or infrastructures to be considered during the closed meeting. A closed meeting must be tape recorded at the expense of the governing body, and the recording must be preserved for at least four years.

13D.06. Civil fines; forfeiture of office; other remedies

Subdivision 1. Personal liability for $300 fine. Any person who intentionally violates this chapter shall be subject to personal liability in the form of a civil penalty in an amount not to exceed $300 for a single occurrence, which may not be paid by the public body.

Subd. 2. Who may bring action; where. An action to enforce the penalty in subdivision 1 may be brought by any person in any court of competent jurisdiction where the administrative office of the governing body is located.

Subd. 3. Forfeit office if three violations.

(a) If a person has been found to have intentionally violated this chapter in three or more actions brought under this chapter involving the same governing body, such person shall forfeit any further right to serve on such governing body or in any other capacity with such public body for a period of time equal to the term of office such person was then serving.

(b) The court determining the merits of any action in connection with any alleged third violation shall receive competent, relevant evidence in connection therewith and, upon finding as to the occurrence of a separate third violation, unrelated to the previous violations, issue its order declaring the position vacant and notify the appointing authority or clerk of the governing body.

(c) As soon as practicable thereafter the appointing authority or the governing body shall fill the position as in the case of any other vacancy.

Subd. 4. Other remedies; requirements; limits.

(a) In addition to other remedies, the court may award reasonable costs, disbursements, and reasonable attorney fees of up to $13,000 to any party in an action under this chapter.

(b) The court may award costs and attorney fees to a defendant only if the court finds that the action under this chapter was frivolous and without merit.

(c) A public body may pay any costs, disbursements, or attorney fees incurred by or awarded against any of its members in an action under this chapter.

(d) No monetary penalties or attorney fees may be awarded against a member of a public body unless the court finds that there was a specific intent to violate this chapter.

13D.07. Citation

This chapter may be cited as the "Minnesota open meeting law."