

Minnesota Attorney General: Administrative Rules Proceedings

Copyright Notice:

This material may be protected by copyright law (U.S. Code, Title 17). Researchers are liable for any infringement. For more information, visit www.mnhs.org/copyright.

Version 3
August 20, 2018

1

SN (R347)

2 MCAR § 1.201. Scope and purpose. These rules relate to and shall apply to the provisions of Minn. Stat. §§ 15.162 through 15.1671.

A. These rules shall apply to those governmental entities as defined by Minn. Stat. § 15.1671, subd. 5, 7, and 8, which collect, create, use, store, and disseminate data on individuals as defined in Minn. Stat. § 15.162, subd. 3.

B. Nonprofit social service agencies meeting the requirements of Minn. Stat. § 15.162, subd. 5 shall include, but are not limited to, agencies providing mental health, physical health, counseling and day-activities services.

1. These rules shall only apply in the instance where such an agency is required, by the terms of a written contract with a state agency, political subdivision, or statewide system to collect, create, store, use, or disseminate data on individuals.

2. In the event of such a contract, these rules shall only apply to the data on individuals that is actually generated by the social service agency because of the contract.

3. Any data generated by activities of the social service agency that are independent of the contractually based activities shall not be subject to these rules.

4. These rules shall not apply to personnel data maintained on employees of such social service agencies.

C. These rules shall not apply to any governmental data collected, created, used, stored, or disseminated which is not data on individuals as defined in Minn. Stat. § 15.162, subd. 3, except these rules shall apply to summary data.

D. Nothing in these rules shall limit the discovery procedures available at law to any party in a civil or criminal action or administrative proceeding as described in the Minnesota Rules of Civil Procedure and the Minnesota Rules of Criminal Procedure as adopted by the Minnesota Supreme Court or in Minnesota Statutes.

E. Nothing in these rules shall restrict or limit the scope or operation of any judicial order or rule issued by a state or federal court.

F. Nothing in these rules shall be construed to diminish the rights conferred on subjects of data by Minn. Stat. § 15.165, or any other statute.

G. The purpose of these rules is to aid governmental entities in implementing and administering Minn. Stat. §§ 15.162 through 15.1671. These rules are intended to guide entities so that while protection is given to individual privacy, neither necessary openness in government nor the orderly and efficient operation of government is curtailed.

Enabling Authority:

15.1671 DUTIES OF THE COMMISSIONER.

The commissioner shall with the advice of the intergovernmental information services advisory council promulgate rules, in accordance with the rule-making procedures in the administrative procedures act which shall apply to state agencies, statewide systems and political subdivisions to implement the enforcement and administration of sections 15.162 to 15.169. The rules shall not affect section 15.165, relating to rights of subjects of data, and section 15.169, relating to the powers and duties of the privacy study commission. 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 15.0412, subdivision 3, of the date and place of hearing, enclosing a copy of the rules and regulations to be adopted.

15.162

Subd. 5. "Political subdivision" means any county, statutory or home rule charter city, school district, special district and any board, commission, district or authority created pursuant to law, local ordinance or charter provision. It includes any nonprofit corporation which is a community action agency organized pursuant to the economic opportunity act of 1964 (P. L. 88-452) as amended, to quality 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. 7. "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. 8. "Statewide system" includes any recordkeeping system in which data on individuals 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.

15.162, Subd. 5

It includes any nonprofit corporation which is a community action agency organized pursuant to the economic opportunity act of 1964 (P. L. 88-452) as amended, to quality 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.

15.162

Subd. 3. "Data on individuals" includes all records, files and processes which contain any data in which an individual is or can be identified and which are retained or intended to be retained on a permanent or temporary basis. It includes data collected, stored, or disseminated by manual, mechanical, electronic or any other means. Data on individuals are classified as public, private or confidential.

201-D

Includes Discovery: Civil Pro. Rule 26.01 et seq.

Trials subpoena 45.02

Criminal Proc.
Depositions - Rule 21
Subpoena - Rule 22

Stat. Authority
15.1691 - admin. of Stat.
Smith v Cnty of Hennepin

Needed to implement rules

Stat. Interp. -
{ Public interest paramount
{ Rts of individuals
gives way
Thrust of Law: openness in government

Case Law
Smith v Cnty of Hennepin
Katz Schade v Lundberg
cards not public / are discoverable

2

S.N. (R 348)

2 MCAR § 1.202

2 MCAR § 1.202 Definitions. All terms shall have the meanings given them by Minn. Stat. § 15.162. Those terms and additional terms as used in these rules shall have the meanings as follows:

A. Act means Minn. Stat. §§ 15.162 through 15.1671, as amended, commonly referred to as the "Data Privacy Act" or the "Minnesota Fair Information Practices Act".

B. Arrest Information means only those elements of data that are expressly listed in § 15.162, subd. 1a of the Act. Arrest information shall only include data which is collected, created, or maintained by an entity whose officers, employees, or agents are given arrest powers by statute, or the power to take into custody any person arrested by another citizen of this state.

1. Such entities include, but are not limited to, municipal police departments, county sheriff departments, the Minnesota State Patrol, and officers deputized as game wardens under the provisions of Minn. Stat. § 97.50.

C. Data means "data on individuals" as defined in § 15.162, subd. 3 of the Act, unless stated otherwise.

1. Data can be maintained in any form, including, but not limited to, paper records and files, microfilm, computer medium, or other processes.

2. The duration of the existence of data, including whether certain data is temporary rather than permanent, is not relevant to compliance with these rules.

3. All data, in whatever form it is maintained, is "data on individuals" if it can in any way identify a unique individual.

4. Code numbers representing unique individuals in certain data constitute "data on individuals", provided a list or index of any type is made available by which the code number can be cross referenced to identify unique individuals. Such data may qualify for treatment as summary data, pursuant to 2 MCAR § 1.209.

a. Code number means the labeling or enumeration of data by use of a letter, number, or combination thereof, which is used in place of an individual's name, including but not limited to index numbers, dummy numbers, SOUNDEX codes, and social security numbers.

5. Data is "data on individuals" if it identifies an individual in itself, or if it can be used in connection with other data elements to uniquely identify an individual. Such data shall include, but is not limited to, street addresses, job titles and so forth where the particular data could only describe or identify one individual.

Arrest Info. - Not Q of legisl. intent except to explain reasonableness of agency's decision.

15.162

Subd. 1a. "Arrest information" shall include (a) the name, age, and address of an arrested individual; (b) the nature of the charge against the arrested individual; (c) the time and place of the arrest; (d) the identity of the arresting agency; (e) information as to whether an individual has been incarcerated and the place of incarceration. "Arrest information" does not include data specifically made private, confidential or nonpublic pursuant to section 260.161 or any other statute.

Juvenile Ct. Records

Phrase reasonably contemporaneous - 15.162 (2a, 5a)

15.162

Subd. 3. "Data on individuals" includes all records, files and processes which contain any data in which an individual is or can be identified and which are retained or intended to be retained on a permanent or temporary basis. It includes data collected, stored, or disseminated by manual, mechanical, electronic or any other means. Data on individuals are classified as public, private or confidential.

3

(R 348)

D. Confidential Data as defined in § 15.162, subd. 2a of the Act, shall only include data which is expressly classified by either a state statute, including the provisions of § 15.1642 of the Act, or federal law.

1. Data is confidential only if a state statute or federal law provides substantially that:

a. Certain data shall not be available either to the public or to the data subject; or

b. Certain data shall not be available to anyone for any reason except agencies which need the data for agency purposes.

2. Data is not confidential if:

a. A state statute or federal law provides that the data is confidential, but the context of the statute or federal law, in which the term confidential appears, reasonably indicates the data is accessible by the data subject.

3. A state agency rule, an executive order, an administrative decision, or a local ordinance shall not classify data as "confidential", or use wording to make data inaccessible to the data subject unless there is a state statute or federal law as the basis for the classification.

E. Private Data, as defined in § 15.162, subd. 5a of the Act, shall only include data which is expressly classified by either a state statute, including the provisions of § 15.1642 of the Act, or federal law.

1. Data is private if a state statute or federal law provides substantially that:

a. Certain data shall not be available to the public but shall be available to the subject of that data;

b. Certain data shall not be available to anyone, except the data subject or his designated representative such as an attorney;

c. Certain data shall be confidential and the person the data is about may view the data at reasonable times; or

d. Certain data shall be confidential and may be shown to the data subject at the discretion of the person holding the data. Such data shall be private if the state statute or federal law does not provide standards which limit the exercise of the discretion of the person maintaining the data.

2. Data is not private if:

a. Absent a statutory or federal law basis for classification, a state agency rule, an executive order, an administrative decision or a local ordinance provides substantially that certain data shall be private, pursuant to Minn. Stat. § 15.162, subd. 5a, or any other similar wording.

b. A federal agency rule provides substantially that as a part of its plan for implementation of a certain federal program, a state agency, statewide system, or political subdivision must provide for the confidentiality of data obtained from program subjects.

15.162

Subd. 2a. "Confidential data on individuals" means data which is: (a) made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data; or (b) collected by a civil or criminal investigative agency as part of an active investigation undertaken for the purpose of the commencement of a legal action, provided that the burden of proof as to whether such investigation is active or in anticipation of a legal action is upon the agency. Confidential data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration. The provision of clause (b) shall terminate and cease to have force and effect with regard to the state agencies, political subdivisions, statewide systems, covered by the ruling, upon the granting or refusal to grant an emergency classification pursuant to section 15.1642 of both criminal and civil investigative data, or on July 31, ~~1978~~ 1979, whichever occurs first.

15.162

Subd. 5a. "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. Private data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration.

4

(R 349)

F. Public Data shall mean "data on individuals", as defined in § 15.162, subd. 5b of the Act, which is neither private nor confidential data, and which is data that is an official record pursuant to Minn. Stat. § 15.17.

1. Data is public if:

a. a state statute or federal law substantially provides that certain data shall be made available to the public, pursuant to Minn. Stat. § 15.17, or any other similar wording;

b. a state statute or federal law substantially requires the collection of certain data by a state agency, political subdivision or statewide system, and does not classify that data as private or confidential;

c. a state agency, statewide system, or political subdivision, without any express enabling authority to do so, collects certain data because that data is necessary to its operations; as defined at 2 MCAR § 1.216 B.1.

P.22 - R359-358

2. This rule shall not limit the ability of an entity to apply for emergency classifications of data pursuant to § 15.1642 of the Act.

G. Designee means any person designated by a responsible authority to be in charge of individual file(s) or system(s) containing "data on individuals". R355- Appointment of Designee

H. Entity means any governmental agency subject to the requirements of the Act, including state agencies, political subdivisions, and statewide systems as those terms are defined in § 15.162 of the Act.

1. State agency shall include any entity which is given power of statewide impact by statute or executive order.

2. Political subdivision shall include those local government entities which are given powers of less than statewide impact by statute or executive order.

3. Statewide systems shall include, but are not limited to, recordkeeping and data administering systems established by statute, federal law, administrative decision or agreement, or joint powers agreement.

a. Statewide systems shall include, but are not limited to, the Criminal Justice Information System administered by the Bureau of Criminal Apprehension, the Statewide Accounting System, the Minnesota Education Computing Consortium, and the various welfare systems primarily administered by the Department of Public Welfare.

I. Federal Law means United States Code, rules of federal agencies as published in the *Federal Register*, and federal case law, including decisions of any court in the federal judicial system.

J. Individual means any living human being. Individual shall not include any fictional entity or business such as a corporation, association, partnership, or sole proprietorship even in those instances where the name of such an entity or business includes the name of a natural person.

K. Records Management Act means Minn. Stat. § 138.17.

15.162

Subd. 5b. "Public data on individuals" means data which is accessible to the public in accordance with the provisions of section 15.17.

15.17 OFFICIAL RECORDS.

Subdivision 1. MUST BE KEPT. All officers and agencies of the state, and all officers and agencies of the counties, cities and towns, shall make and keep all records necessary to a full and accurate knowledge of their official activities. All such public records shall

Subd. 4. ACCESSIBLE TO PUBLIC. Every custodian of public records shall keep them in such 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. Except as otherwise expressly provided by law, he shall permit all public records in his custody to be inspected, examined, abstracted, or copied at reasonable times and under his supervision and regulation by any person; and he shall, upon the demand of any person, furnish certified copies thereof on payment in advance of fees not to exceed the fees prescribed by law. 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 public records except as otherwise expressly provided by law.

15.162

Subd. 5. "Political subdivision" means any county, statutory or home rule charter city, school district, special district and any board, commission, district or authority created pursuant to law, local ordinance or charter provision.

Subd. 7. "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. 8. "Statewide system" includes any recordkeeping system in which data on individuals 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.

15.162, subd 5a

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

15.162

Subd. 4. "Individual" means a natural person. In the case of a minor, "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.

not natural person

5/
(R 349)

15.162

Subd. 6. "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 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 or summary data, unless otherwise provided by state law.

See R 355 for Appointment of R/A

L. Responsible Authority means the individual in each entity who is designated or appointed pursuant to § 15.162, subd. 6 of the Act.

1. In state agencies, the Responsible Authority shall be as follows:

a. Departments: the commissioner of the department.

b. Constitutional Offices: the constitutional officer.

c. University of Minnesota: the individual appointed by the Board of Regents.

d. All other state agencies: the chief executive officer, or if none, then an individual chosen by the agency's governing body.

2. In political subdivisions, the Responsible Authority shall be as follows:

a. Counties: each elected official of the county shall be the Responsible Authority for his respective office. An individual who is an employee of the county shall be appointed by the county board to be the Responsible Authority for any data administered outside the offices of elected officials.

b. Cities: the city council shall appoint an individual who is an employee (or officer) of the city.

c. School Districts: the school board shall appoint an individual who is an employee of the school district.

d. Nonprofit Corporations or Nonprofit Social Service Agencies: unless a statute or the governmental entity which created the corporation or agency appoints an individual, the governing body of the corporation or agency shall appoint an individual. If no appointment is made, the chief executive officer of the nonprofit corporation or agency shall be the Responsible Authority. If the corporation or agency is part of a statewide system, the Responsible Authority for the statewide system shall be the Responsible Authority for the corporation or agency as determined by this rule.

e. All other political subdivisions: the governing body shall appoint an individual who is an employee of the political subdivision.

3. In Statewide Systems, the Responsible Authority shall be as follows:

a. The commissioner of any state department or any executive officer designated by statute or executive officer designated by statute or executive order as responsible for such a system; or

b. If a state statute or executive order does not designate an individual as Responsible Authority, the Commissioner of Administration shall appoint the Responsible Authority after the entities which participate in the system jointly apply for such an appointment in a form provided by the Commissioner of Administration.

6

(R 350)

15.162

M. Summary Data, as defined in § 15.162, subd. 9 of the Act, means data which has been extracted, manipulated, or summarized from private or confidential data, and from which all data elements that could link the data to a specific individual have been removed.

1. Summary data includes, but is not limited to, statistical data, case studies, reports of incidents, and research reports.

2. Data is summary data if any list of numbers or other data which could uniquely identify any individual in the summary data is physically separated from the summary data and is not made available to persons who gain access to, or possession of the summary data.

Subd. 9. "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.

7

(R 350)

2 MCAR § 1.203 Access to Public Data. The Responsible Authority shall comply with the following general rules governing access to public data.

A. The Responsible Authority shall provide access to public data to any person, regardless of that person's interest in the data.

1. The Responsible Authority shall establish procedures to describe how such access may be gained.

a. In such procedures, the Responsible Authority may limit the time that public access is available to the normal office hours of the agency.

b. In such procedures, the Responsible Authority shall provide for a response to a request for access within a reasonable time.

c. The Responsible Authority shall charge a reasonable fee for providing copies of public data unless the costs incurred by the entity in providing the copies are minimal.

d. In determining the amount of the reasonable fee, the Responsible Authority shall be guided by the following:

(1.) The cost of materials, including paper, used to provide the copies.

(2.) The cost of the labor required to prepare the copies.

(3.) Any schedule of standard copying charges as established by the agency in its normal course of operations.

(4.) Any special costs necessary to produce such copies from machine based record keeping systems, including but not limited to computers and microfilm systems.

(5.) Mailing costs.

15.162

Subd. 5b. "Public data on individuals" means data which is accessible to the public in accordance with the provisions of section 15.17.

15.17 OFFICIAL RECORDS.

Subdivision 1. MUST BE KEPT. All officers and agencies of the state, and all officers and agencies of the counties, cities and towns, shall make and keep all records necessary to a full and accurate knowledge of their official activities. All such public records shall

Subd. 4. ACCESSIBLE TO PUBLIC. Every custodian of public records shall keep them in such 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. Except as otherwise expressly provided by law, he shall permit all public records in his custody to be inspected, examined, abstracted, or copied at reasonable times and under his supervision and regulation by any person; and he shall, upon the demand of any person, furnish certified copies thereof on payment in advance of fees not to exceed the fees prescribed by law. 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 public records except as otherwise expressly provided by law.

Access - dictionary def. - using =>

8

(R 350)

15.162

Subd. 5a. "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. Private data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration.

2 MCAR § 1.204 Access to private data. Pursuant to §§ 15.1641 and 15.162, subd. 5a of the Act, the Responsible Authority shall comply with the following rules concerning access to private data:

A. Access to private data shall be available only to the following:

1. The subject of such data.

2. Individuals within the entity, whose work assignments reasonably require access.

3. Entities and agencies as determined by the Responsible Authority who are authorized by statute, including § 15.1641 (e) of the Act, or federal law to gain access to that specific data.

4. Entities or individuals given access by the express written direction of the data subject.

B. The Responsible Authority shall establish written procedures to assure that access is gained only by those parties identified in Part A of the rule.

1. In those procedures, the Responsible Authority shall provide for reasonable measures that will assure that the person seeking to gain access to the private data is actually the subject of that data or the authorized representative of the data subject.

2. Such reasonable measures include, but are not limited to, the following:

a. Requiring the person seeking to gain access to appear at the offices of the entity to gain such access or requiring the notarized signature of any data subject who is unable to appear at the offices of the entity.

→ Possible confl. w/ A-4-

b. Requiring the person to provide reasonable identification.

C. The Responsible Authority may limit the time that access is available to the data subject to the normal working hours of the agency.

D. The Responsible Authority shall not charge the data subject any fee in those instances where the data subject only desires to view private data.

E. The Responsible Authority shall charge the data subject a reasonable fee for providing copies of private data.

1. In determining the amount of the reasonable fee, the Responsible Authority shall be guided by the criteria set out in 2 MCAR § 1.203 concerning access to public data.

(R 351)

9

15.162

2 MCAR § 1.205 Access to private data concerning data subjects who are minors. Pursuant to §§ 15.1641 and 15.162, subd. 4 and 5a of the Act, the Responsible Authority shall comply with the following rules concerning access:

Except as provided in this rule...

A. In addition to the particular requirements of this rule, access to private data concerning a minor data subject shall be subject to the requirements of 2 MCAR § 1.204 concerning access to all private data.

B. Access to private data concerning minors shall be available only to the following:

1. Those parties identified as having access to private data under part A. of 2 MCAR § 1.204.

2. Subject to the provisions of Minn. Stat. § 15.162, subd. 4, any other applicable statute, and the exception set out at subd. C.1. below, the parents of the minor data subject.

a. For purposes of this rule, the Responsible Authority shall presume the parent has the authority to exercise the rights inherent in the Act unless the Responsible Authority has been provided with evidence that there is a state law or court order governing such matters as divorce, separation, or custody, or a legally binding instrument which provides to the contrary.

C. Pursuant to the provisions of Minn. Stat. § 15.162, subd. 4, the Responsible Authority shall establish procedures to provide access by the parents of a minor data subject to private data concerning that minor, subject to the following:

Subject to the provisions of subd. 2 (above)

1. The Responsible Authority may deny parental access to private data when the minor, who is the subject of that data, requests that the Responsible Authority deny such access.

a. The Responsible Authority may require the minor data subject to submit a written request that the data be withheld. The written request shall set forth the reasons for denying parental access and shall be signed by the minor.

2. Upon receipt of such a request, the Responsible Authority shall determine if honoring the request to deny parental access would be in the best interest of the minor data subject.

a. In making the determination, the Responsible Authority shall be guided by at least the following:

(1) Whether the minor is of sufficient age and maturity to be able to explain the reasons for and to understand the consequences of the request to deny access.

(2) Whether the personal situation of the minor is such that denying parental access may protect the minor data subject from physical or emotional harm.

(3) Whether there is ground for believing that the minor data subject's reasons for precluding parental access are reasonably accurate.

(4) Whether the data in question is of such a nature that disclosure of it to the parent could lead to physical or emotional harm to the minor data subject.

(5) Whether the data in question is subject to the right of parental access outlined in the "Family Educational Rights and Privacy Act of 1974," Public Law 93-380, and the rules promulgated thereunder.

(6) Whether the data concerns medical, dental or other health services provided pursuant to Minn. Stat. §§ 144.341 through 144.347. If so, the data may be released only if failure to inform the parent would seriously jeopardize the health of the minor.

→ Whether failure to inform the parent would seriously jeopardize the health of the minor when the data concerns medical, dental or other health services...

Subd. 4. "Individual" means a natural person. In the case of a minor, "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.

5a - private data definition

.1641 - (c) Duties of R/A re private + conf. data

Minn Stat 260.161 et seq

Says legal records open to minor + parent — not public — so it is private.

10

15.162

S.A. Post (R 352)

14

2 MCAR § 1.206 Access to confidential data. Pursuant to Minn. Stat. §§ 15.1641 and 15.162, subd. 2a, the Responsible Authority shall comply with the following rules concerning access to confidential data:

A. Access to confidential data is available only to the following:

1. Individuals within the entity, whose work assignments reasonably require access.

2. Entities and agencies who are authorized by statute, including § 15.1641 of the Act, or federal law to gain access to that specific data.

B. The Responsible Authority shall establish written procedures to assure that access may be gained only by those parties identified in Part A. of this rule.

1. In the drafting and administration of those procedures, the Responsible Authority shall provide measures by which data subjects shall be informed, upon request, if they are the subjects of confidential data.

a. The Responsible Authority shall not disclose the actual confidential data to the data subjects, but shall inform them whether confidential data concerning them is or is not retained.

b. The Responsible Authority shall take reasonable measures to assure that the person making inquiry is actually the individual data subject.

c. Reasonable measures may include, but are not limtied to:

(1) Requiring the inquiring person to appear at the office of the entity to make his/her request.

(2) Requiring the inquiring person to provide identification.

(3) Requiring the notarized signature of any data subject who is unable to appear at the offices of the entity.

Subd. 2a. "Confidential data on individuals" means data which is: (a) made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data; or (b) collected by a civil or criminal investigative agency as part of an active investigation undertaken for the purpose of the commencement of a legal action, provided that the burden of proof as to whether such investigation is active or in anticipation of a legal action is upon the agency. Confidential data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration. The provision of clause (b) shall terminate and cease to have force and effect with regard to the state agencies, political subdivisions, statewide systems, covered by the ruling, upon the granting or refusal to grant an emergency classification pursuant to section 15.1642 of both criminal and civil investigative data, or on July 31, 1978 1979, whichever occurs first.

11

(R 352)

2 MCAR § 1.207 Access to arrest information. Pursuant to § 15.162, subd. 1a, 2a, and 5a of the Act, the Responsible Authority shall comply with the following rules concerning access to arrest information:

A. For the duration of time, defined in Part B of this rule, that immediately follows the creation of data constituting arrest information, the Responsible Authority shall make such information available to anyone who requests it in writing, by personal appearance, by telephone inquiry, or any other means.

B. For purposes of this rule, "duration of time" commences with the creation or recording of the arrest information subsequent to the actual detention or citation of the arrested party. "Duration of time" ends at that point in time when an arrested party is:

1. Either released without a criminal complaint being filed against him/her; or

2. Appears before a judicial officer for the offense for which he/she was arrested, or any lesser included offense as described in the Rules of Criminal Procedure as adopted by the Minnesota Supreme Court.

C. During the duration of time described in Part B. of this rule, the Responsible Authority shall not be limited to publicly releasing only arrest information, as defined by § 15.162, subd. 1a of the Act. The Responsible Authority may release additional information after consideration of at least the following:

1. Whether the status afforded to certain data as investigative data, pursuant to § 15.162, subd. 2a of the Act, is no longer needed to protect the integrity of an investigation.

2. Whether there is concern and interest on the part of the public in the person arrested or the alleged crime committed.

3. Whether the release of additional data and its subsequent publication may prejudice the arrested individual's right to a fair and impartial trial.

4. Whether the data subject has requested that arrest disposition data pertaining to that data subject be disseminated.

5. Whether the identity of any victims of or witnesses to the crime should be protected.

D. The Responsible Authority shall not make available to the public any data concerning the detention of a juvenile individual, unless that juvenile is judicially certified to be tried as an adult as described in the Minnesota Rule of Criminal Procedure. The Responsible Authority shall make any data concerning the detention of a juvenile available to the parents of the juvenile.

15.162

Subd. 1a. "Arrest information" shall include (a) the name, age, and address of an arrested individual; (b) the nature of the charge against the arrested individual; (c) the time and place of the arrest; (d) the identity of the arresting agency; (e) information as to whether an individual has been incarcerated and the place of incarceration. "Arrest information" does not include data specifically made private, confidential or nonpublic pursuant to section 260.161 or any other statute.

Definition - page 2

15.162

Subd. 2a. "Confidential data on individuals" means data which is: (a) made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data; or (b) collected by a civil or criminal investigative agency as part of an active investigation undertaken for the purpose of the commencement of a legal action, provided that the burden of proof as to whether such investigation is active or in anticipation of a legal action is upon the agency. Confidential data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration. The provision of clause (b) shall terminate and cease to have force and effect with regard to the state agencies, political subdivisions, statewide systems, covered by the ruling, upon the granting or refusal to grant an emergency classification pursuant to section 15.1642 of both criminal and civil investigative data, or on July 31, 1978 1979, whichever occurs first.

Subd. 5a. "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. Private data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration.

AG Opinion 8/2/76
It is not the request which must be "reasonably contemporaneous" but the information. Thus the info would always be public.

C. - Within purview of discretion of r.a. vis a vis investigative data.

12

(R 353)

Is there discretion for investigative data? - How will/can it be?

2 MCAR § 1.208 Access to Investigative Data. Pursuant to Minn. Stat. §§ 15.162, subd. 2a and 15.1641 of the Act, the Responsible Authority shall comply with the following general rules concerning access to investigatory data:

A. Investigatory data is confidential data, pursuant to § 15.162, subd. 2a(b). The Responsible Authority shall comply with the provisions of 2 MCAR § 1.206, concerning access to confidential data.

B. The Responsible Authority shall determine that data maintained by his entity is investigative data only if all criteria set out in Parts 1, 2, and 3 of this section are met.

1. Collecting agency criteria. The data is collected, created, or maintained by or at the direction of one of the following entities, or by an agent of such entity:

a. Law enforcement agencies, whose agents are given arrest powers, including, but not limited to, those entities listed in 2 MCAR § 1.201 B.1.

b. Public attorneys, who are given the statutory or constitutional authority to prosecute or to defend civil or criminal actions as defined by the Minnesota Rules of Civil Procedure and the Minnesota Rules of Criminal Procedure including, but not limited to, municipal and county prosecutors and members of the Attorney General's staff.

c. Judicial entities, whose agents are given the statutory or constitutional authority to adjudicate cases and to render sentences.

d. Any agency given statutory authority to revoke or suspend licensure.

e. Any entity which has a reasonable expectation that certain data in its possession may become the subject of a legal action, as set forth in Part 2 of this section.

2. Purpose of collection criteria. The data is collected or created for the purpose of the commencement of a legal action. Any of the following shall constitute a "legal action", for the purposes of this rule, and as used in Minn. Stat. § 15.162, subd. 2a(b):

a. Arrest of any individual.

b. Issuance of a citation, complaint, or an indictment as described in Minnesota Rules of Criminal Procedure.

c. Service of a civil complaint on behalf of the state, a state agency, or a political subdivision.

d. Service of a civil answer on behalf of the state, a state agency, or a political subdivision.

e. Maintaining or prosecuting a civil or criminal action on behalf of the state, a state agency, or political subdivision.

f. Conducting any arbitration proceeding pursuant to Minn. Stat. ch. 572.

g. Conducting any proceeding which may lead to the suspension or revocation of any type of license issued by a state agency or political subdivision.

3. Active data criteria. Active data includes:

a. Data collected for the purpose of the commencement of a criminal action in which all perpetrators of the criminal violation have not been apprehended, the matter has not been fully adjudicated, the statute of limitations for the alleged violation has not run, or all rights of appeal in the judicial system have not been exhausted.

b. Data collected for the purpose of bringing or defending a civil action where that action has not been finally resolved, including exhaustion or extinguishment of all rights of appeal in the judicial system.

c. Data collected for the purpose of participation in an arbitration proceeding where that proceeding has not resulted in a binding decision, including exhaustion of all rights of appeal in the judicial system.

d. Data collected for the purpose of participation in a license revocation or suspension proceeding where that proceeding has not resulted in a binding decision, including exhaustion of all rights of appeal in the judicial system.

15.162

Subd. 2a. "Confidential data on individuals" means data which is: (a) made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data; or (b) collected by a civil or criminal investigative agency as part of an active investigation undertaken for the purpose of the commencement of a legal action, provided that the burden of proof as to whether such investigation is active or in anticipation of a legal action is upon the agency. Confidential data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration. The provision of clause (b) shall terminate and cease to have force and effect with regard to the state agencies, political subdivisions, statewide systems, covered by the ruling, upon the granting or refusal to grant an emergency classification pursuant to section 15.1642 of both criminal and civil investigative data, or on July 31, 1978 1979, whichever occurs first.

Even if "reasonably contemporaneous" failed as being improper interp., def of investigative data OK. → 2 Qs: is where is the discretion to kick pursuant section refers?

13

(R 354)

2 MCAR § 1.209 Access to Summary Data. Pursuant to Minn. Stat. § 15.641 (d), the Responsible Authority shall comply with the following general rules concerning access to summary data:

A. Summary data is public data. The Responsible Authority shall comply with 2 MCAR § 1.203, concerning access to public data.

B. The Responsible Authority shall prepare and implement procedures in his/her agency to assure that access to summary data is given to anyone who requests such data. In the preparation and administration of such procedures, the Responsible Authority shall comply with the following:

1. Preparation of summary data may be requested by any person. The request shall be in writing in a form provided by the Responsible Authority. Within ten days of the receipt of such a request, the Responsible Authority shall inform the requestor of the estimated costs if any, pursuant to subd. B.2 of this rule and subject to the provisions of that subd., either:

a. Provide the summary data requested; or

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

c. Provide access to the requestor to the private or confidential data for the purpose of the requestor's preparation of summary data, pursuant to § 15.1641 (d) of the Act and subd. B.4. of this rule.

2. Any costs incurred in the preparation of summary data shall be borne by the requesting person. In assessing the costs associated with the preparation of summary data, the Responsible Authority shall:

a. Be guided by the provisions of 2 MCAR § 1.203 in determining costs.

b. Provide to the requesting person an estimate of the costs associated with the preparation of the summary data.

c. Prior to preparing or supplying the summary data, collect any funds necessary to reimburse the entity for its costs.

d. Charge no more than reasonable copying costs when the summary data being requested requires only copying and no other preparation.

e. Take into account the reasonable value to the entity of the summary data prepared.

3. For the purposes of administering Minn. Stat. § 15.1641 (d), the following terms shall have the meanings given them.

a. "Administrative officer" includes, but is not limited to, the entity's research director, statistician, or computer center director.

b. "Person outside" the entity includes the person requesting the summary data or any other person designated by the person requesting the data.

15.162

Subd. 9. "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.

15.1641

(d) The use of summary data derived from private or confidential data on individuals under jurisdiction of one or more responsible authorities shall be permitted, provided that summary data is public pursuant to section 15.17. The responsible authority shall prepare summary data from private or confidential data on individuals upon the request of any person, provided that the request is in writing and the cost of preparing the data is borne by the requesting person. The responsible authority may delegate the power to prepare summary data to the administrative officer responsible for any central repository of summary data, or to a person outside of its agency if the person agrees in writing not to disclose private or confidential data on individuals.

(R 354)

4. A nondisclosure agreement, as required by § 15.1641 (d) of the Act, shall contain at least the following:

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

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

c. A statement that the preparer understands he/she may be subject to the civil or criminal penalty provisions of the Act in the event that the private or confidential data is disclosed.

5. Methods of preparing summary data include, but are not limited to, the following:

a. Removing from a set of data, a file, or a record keeping system all unique personal identifiers so that the data that remains fulfills the definition of summary data as defined by § 15.162, subd. 9 of the Act.

b. Removing from the entity's report of any incident, or from any collection of data similar to an incident report, all unique personal identifiers so that the resulting report fulfills the definition of summary data in § 15.162, subd. 9 of the Act.

c. For purposes of this rule, "removing all unique personal identifiers" includes but is not limited to:

(1) Blacking out personal identifiers on paper records.

(2) Tearing off or cutting out the portions of paper records that contain the personal identifiers.

(3) Programming computers in such a way that printed or terminal output does not contain personal identifiers.

15.162

Subd. 9. "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.

15.1641

(d) The use of summary data derived from private or confidential data on individuals under jurisdiction of one or more responsible authorities shall be permitted, provided that summary data is public pursuant to section 15.17. The responsible authority shall prepare summary data from private or confidential data on individuals upon the request of any person, provided that the request is in writing and the cost of preparing the data is borne by the requesting person. The responsible authority may delegate the power to prepare summary data to the administrative officer responsible for any central repository of summary data, or to a person outside of its agency if the person agrees in writing not to disclose private or confidential data on individuals.

q - why include pupose?

15

(R 355)

2 MCAR § 1.210 Classification of data. In order to comply with the provisions of §§ 15.162, 15.1641, 15.165 and 15.163 of the Act the Responsible Authority shall:

A. Review and identify all of the types of data maintained by the entity, including data retained as active and inactive.

B. Determine the private, confidential, or public classification for each type of data, according to the definitions of those terms pursuant to § 15.162 of the Act and 2 MCAR § 1.202.

C. Identify either a state statute or provisions of federal law supporting any determination that certain data is either private or confidential.

B. Administer all agency data in accordance with the determinations made under 2 MCAR § 1.210 B.

Need Authority - what sections help?

Min Stat 15.162, subd 3.
"'Data on individuals' includes all records, files + processes .... Data on individuals are classified as public, private or confidential."

M.S. 15.162 subd 6
"R.A. .... responsible for collection, use and dissemination .... "

MS 15.1671
".... implement the enforcement + administration of ... "

16

(R 355)

2 MCAR § 1.211 Authority of the Responsible Authority. Jurisdiction, as that term is used in § 15.1641 (a) of the Act, means that the Responsible Authority shall have the authority to:

SN

20

A. Implement the Act and these rules in each entity.

B. Make good faith attempts to resolve all administrative controversies arising from the entity's practices of creation, collection, use, and dissemination of data.

C. Prescribe changes to the administration of the entity's programs, procedures, and design of forms to bring those activities into compliance with the Act and with these rules.

D. Take all administrative actions necessary to comply with the general requirements of the Act, particularly Minn. Stat. § 15.165, and these rules.

E. Where necessary, direct designees to perform the detailed requirements of the Act and these rules under the general supervision of the Responsible Authority.

15.1641 DUTIES OF RESPONSIBLE AUTHORITY.

(a) Data on individuals is under the jurisdiction of the responsible authority who may appoint an individual to be in charge of each file or system containing data on individuals.

17

(R 355)

2 MCAR § 1.212 Appointment of the Responsible Authority.

A. Pursuant to § 15.162, subd. 6 of the Act, the governing body of each political subdivision and the governing body of each state agency whose activities are subject to the direction of a governing body shall, within 30 days of the effective date of these rules, appoint a Responsible Authority.

1. This rule shall not affect the appointments of Responsible Authorities made previous to the adoption of this rule.

2. The governing body shall confer on the Responsible Authority full administrative authority to carry out the duties assigned by the Act and by these rules.

3. Governing bodies may use the forms set forth in the appendix to these rules to appoint the Responsible Authority.

15.162

Subd. 6. "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 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 or summary data, unless otherwise provided by state law.]

See R. 349 for def. of R./A.

18

(R 355)

2 MCAR § 1.213 Appointment power of the Responsible Authority. Pursuant to § 15.1641 (a) of the Act, the Responsible Authority shall, if he deems it to be in the best interest of the administration and enforcement of the Act, appoint designees who shall be members of the staff of the entity. In the exercise of this appointment power, the Responsible Authority shall comply with the following:

A. The appointment order shall be in writing and copies of the order constitute public data on individuals, pursuant to Minn. Stat. § 15.162, subd. 5(b) of the Act.

B. The Responsible Authority shall instruct any designees in the requirements of the Act and of these rules. If the Responsible Authority deems it necessary, such instruction shall include:

1. Distribution to designees of written materials describing the requirements of the Act and of these rules.

2. Preparation of training programs whose objective is to familiarize agency personnel with the requirements of the Act and of these rules.

3. Requiring attendance of designees and other entity personnel at training programs held within or outside the entity.

15.1641 DUTIES OF RESPONSIBLE AUTHORITY.

(a) Data on individuals is under the jurisdiction of the responsible authority who may appoint an individual to be in charge of each file or system containing data on individuals.

R. 349 - Defintion of designee

Classification by rule?

19

(R 355)

2 MCAR § 1.214 Duties of the Responsible Authority relating to public accountability. Pursuant to § 15.163 of the Act, the duties of the Responsible Authority shall include, but not be limited to, the following:

A. For the purposes of public accountability, the Responsible Authority shall, within sixty days of the effective date of these rules, or until August 1 of each year when the requirements of subd. B. of this rule are fully complied with, place his/her name, job title and business address, and the name(s) and job titles of any designees selected by the Responsible Authority on a document.

1. Such document shall be made available to the public and/or posted in a conspicuous place in each entity.

2. The document shall identify the Responsible Authority or designees as the persons responsible for answering inquiries from the public concerning the provisions of the Act or of these rules.

B. In the public document to be prepared or updated by August 1 of each year as required by § 15.163 of the Act, the Responsible Authority shall identify and describe all records, files, or processes maintained by his entity, which contain private or confidential data.

1. In addition to the items to be placed in the public document as required by § 15.163 of the Act, the Responsible Authority shall include the following:

a. The name, title, and address of designees appointed by the Responsible Authority.

b. Identification of the files or systems for which each designee is responsible.

c. A citation of the state statute or federal law which classifies the data as private or confidential.

2. The Responsible Authority shall draft the descriptions of records, files, and processes in easily understandable English. Technical or uncommon expressions, understandable only by a minority of the general public, shall be avoided except where required by the subject matter.

3. The Responsible Authority may use the form set forth in the appendix to these rules to prepare this public document.

15.163 REPORTS TO THE LEGISLATURE.

Subdivision 1. On or before August 1, 1976, the responsible authority shall prepare a public document containing his 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 his state agency, statewide system, or political subdivision. 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 keep it accurate.

Subd. 2. 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.

Next rule 2 MCAR § 1.215 C-1- requires additional info.

20

(R 356)

2 MCAR § 1.215 Duties of the Responsible Authority relating to the administration of Private and Confidential Data. In order to administer the requirements of § 15.1641 (c) of the Act, the Responsible Authority shall determine for each record, file, or process identified in 2 MCAR § 1.214 whether the data contained therein was collected prior or subsequent to August 1, 1975.

A. For each category of record, file, or process containing data collected prior to August 1, 1975, the Responsible Authority shall:

1. Review the federal, state or local legal enabling authority which mandated or necessitated the collection of the private or confidential data.

2. Based on that review, determine the lawful purpose for the collection of the data at the time it was originally collected.

3. Direct the staff of the entity that private or confidential data collected prior to August 1, 1975, shall not be used, stored, or disseminated for any purpose, unless that purpose is authorized by the enabling authority.

B. For each category of record, file, or process containing private or confidential data collected subsequent to August 1, 1975, the Responsible Authority shall:

1. Review the legal enabling authority which mandates or necessitates the collection of the data.

2. Identify the purposes for the collection of and the intended uses of all private or confidential data that have been communicated to data subjects or should have been communicated to data subjects at the time of data collection, pursuant to § 15.165, subd. 2 of the Act.

C. Using the purposes and uses identified in subds. A. and B. of this rule, the Responsible Authority shall:

1. Prepare lists which identify the uses of and purposes for the collection of private or confidential data for each type of record, file, or process identified in 2 MCAR § 1.214.

a. Each list shall identify all persons, agencies, or entities authorized by state or federal law to receive any data disseminated from the particular record, file or process.

2. Pursuant to § 15.165, subd. 2 of the Act, either:

a. Attach each list identifying purposes, uses and recipients of data to all agency forms which collect the private and confidential data that will be retained in each record, file or process; or

b. Communicate, in any reasonable fashion, the contents of each list to data subjects at the time particular data that will be retained in each record, file, or process is collected from them. For purposes of this section, "reasonable fashion" shall include, but not be limited to:

(1) Oral communications made to data subjects.

(2) Providing data subjects with brochures that describe the entity's purposes for the collection of and the uses to be made of private and confidential data.

(c) Private or confidential data on individuals shall not be used, collected, stored or disseminated for any purposes other than those stated to an individual at the time of collection in accordance with section 15.165 or, in the case of data collected prior to August 1, 1975, for any purpose other than those originally authorized by law, unless (1) the responsible authority files a statement with the commissioner describing the purpose and necessity of the purpose with regard to the health, safety or welfare of the public and the purpose is approved by the commissioner, or (2) the purpose is subsecuently authorized by the state or federal legislature, or (3) the purpose is one to which the individual subject or subjects of the data have given their informed consent.

15.165 RIGHTS OF SUBJECTS OF DATA.

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

Subd. 2. An individual asked to supply private or confidential data concerning himself shall be informed of: (a) the purpose and intended use of the requested data within the collecting state agency, political subdivision or statewide system; (b) whether he may refuse or is legally required to supply the requested data; (c) any known consequence arising from his 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.

does not have to be in writing.

21

(R 356-357)

D. In administering the entity's private or confidential data consistent with the provisions of the rules, the Responsible Authority shall:

1. Educate entity personnel as to authorized purposes and uses.

2. Prepare administrative procedures that will acquaint entity personnel with authorized purposes and uses.

3. Distribute policy directives requiring compliance with the entity's determination of authorized purposes and uses.

E. The Responsible Authority shall authorize a new purpose for the collection of private or confidential data or a new use for private or confidential data under any one of the following conditions:

1. If passage of federal or state legislation requires initiation of a new or different purpose or use pursuant to § 15.1641 (c) (2) of the Act; or

2. The Responsible Authority, prior to initiation of the new or different purpose or use, complies with the provisions of either § 15.1641 (c) (1) or (3) of the Act.

a. For the purposes of administration of Minn. Stat. § 15.1641 (c) (1), the Responsible Authority shall file a statement on a form provided by the Commissioner of Administration. A Responsible Authority shall not initiate a new or different purpose or use of private or confidential data until the Responsible Authority receives written approval from the Commissioner of Administration.

b. For the purposes of Minn. Stat. § 15.1641 (c) (3) the following term shall have the meaning given it:

(1) "Informed consent" means the data subject possesses and exercises sufficient mental capacity to make a decision which reflects an appreciation of the consequences of allowing the entity to initiate a new purpose or use of the data in question.

c. For the purposes of the administration of Minn. Stat. § 15.1641 (c) (3), the Responsible Authority shall comply with the following:

(1) The Responsible Authority shall not take any action to coerce any data subject to give an "informed consent." The Responsible Authority shall explain the necessity for or consequences of the new or different purpose or use.

(2) All informed consents shall be given in writing. Prior to any signature being affixed to it by the data subject, such writing shall identify the consequences of the giving of informed consent.

(3) If the Responsible Authority makes reasonable efforts to obtain the informed consent of a data subject and if those efforts are not acknowledged in any way, the Responsible Authority shall interpret the silence of the data subject as the giving of an implied consent to the new or different purpose or use of the data.

(a) For purposes of this section, "reasonable efforts" shall include:

(i) Depositing in the United States Mail, postage pre-paid and directed to the last known address of the data subject, at least two communications requesting informed consent.

(ii) Waiting for a period of not less than 60 days for a response to the second request.

(4) The data subject may give informed consent to less than all of the data elements in any list of data elements presented by a Responsible Authority, thereby giving only partial consent.

(a) Only those elements that the data subject has expressly consented to shall become part of the new or different purpose or use.

15.1641

(c) Private or confidential data on individuals shall not be used, collected, stored or disseminated for any purposes other than those stated to an individual at the time of collection in accordance with section 15.165 or, in the case of data collected prior to August 1, 1975, for any purpose other than those originally authorized by law, unless (1) the responsible authority files a statement with the commissioner describing the purpose and necessity of the purpose with regard to the health, safety or welfare of the public and the purpose is approved by the commissioner, or (2) the purpose is subsequently authorized by the state or federal legislature, or (3) the purpose is one to which the individual subject or subjects of the data have given their informed consent.

What if cannot get informed consent "because no mental capacity? May not be problem

22

(R 357-358)

2 MCAR § 1.216 Duties of the Responsible Authority as they relate to the administration of all Entity Data. Pursuant to § 15.1641 (b) of the Act, the Responsible Authority shall, within eighteen months of the effective date of these rules, formulate a plan that will provide for the review and analysis of the data administration practices of the entity.

A. In the formulation of this plan, the Responsible Authority shall at least provide for the preparation of a list of or index to all data or types of data currently collected, stored, used, or disseminated by the entity.

1. The list or index developed shall include the identification of the state statute(s), federal law(s), or local ordinance(s) that authorize(s) the programs or functions for which data is collected, or which authorize(s) the actual data collection, storage, use or dissemination.

a. The plan shall further provide for the list or index to be updated when new or different data collection, storage, use, or dissemination is authorized.

b. This list or index shall be available to members of the general public, upon request.

B. The Responsible Authority shall use this plan and the list or index developed to aid in the determination of whether collection and storage of data and use and dissemination of private and confidential data is necessary.

1. For purposes of this section, data is necessary if:

a. The particular data is both:

(1) Required to carry out programs and functions that are expressly or impliedly authorized by a provision of state statute, federal law or a local ordinance; and

(2) Periodically examined, updated, modified or referred to by the entity; or

b. The entity would be unable to fulfill its duties without undue or increased burden or expense, if the particular data were not collected, stored, used or disseminated; or

c. Retention of the particular data is required in the event that a legal action is brought against or by the entity; or

d. Retention of the particular data is essential to comply with a state or federal requirement that data be retained for a specified period for the purposes of auditing, records retention, historical interest, and other similar purposes.

C. For any data determined to be not necessary pursuant to subd. B., of this rule, the Responsible Authority shall provide for the following activities in the entity's plan.

1. Taking all actions which include making changes to forms designs, rewriting procedures, and so forth, to assure that all such data is no longer collected and stored and all such private and confidential data is no longer used and disseminated. Private data shall continue to be disseminated upon request by the data subject.

2. Disposing of such data pursuant to the procedures of the Records Management Act.

a. Inquiries concerning procedures for disposition of data may be directed to the Records Management Division, Department of Administration, St. Paul, Minnesota, 55155.

D. In the formulation of the plan described in subd. A. of this rule, the Responsible Authority shall provide for the establishment of administrative mechanisms and procedures that comply with § 15.1641 (e) of the Act. For purposes of this subdivision.

1. "Accurate" means that the data in questions is reasonably correct and free from error.

2. "Complete" means that the data in question reasonably reflects the history of an individual's transactions with the particular entity. Omissions in an individual's history that place the individual in a false light shall not be permitted.

3. "Current" means that the data in question must be logically related to the entity's required and actual use of the data in its day-to-day operations.

15.1641

(b) Collection and storage of public, private or confidential data on individuals and 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, local governing body or mandated by the federal government.

15.1641

(e) The responsible authority shall establish procedures and safeguards to ensure that all public, private or confidential data on individuals is accurate, complete and current.

23

(R 358)

15.1641 (e)

2 MCAR § 1.217 Duties of the Responsible Authority as they relate to computerized data. For the purposes of the administration of § 15.1641 (e) of the Act, the Responsible Authority shall be guided by the following:

A. "Directly accessible files" means files maintained by any entity which contain private or confidential data, to which access can be made or updating performed through the use of any type of communication terminal, including, but not limited to, teletypewriters and cathode ray tube terminals.

B. Within 180 days of the effective date of these rules, the Responsible Authority shall perform an audit of the physical and software security measures that the entity has installed to protect the integrity of "directly accessible files."

C. The nature and extent of the audit shall be at the discretion of the Responsible Authority, subject to the following:

1. The audit shall emphasize a review of any measures taken to assure that private or confidential data is not accessible to the public through the use of a communications terminal.

2. The audit shall include a review of the measures taken to assure all of the entity's computer based data is protected from tampering by unauthorized persons.

D. If it reasonably appears to the Responsible Authority that there are weaknesses in the entity's data security procedures, the Responsible Authority shall:

1. Provide for terminal security and system and data integrity through the establishment of appropriate security measures.

a. Appropriate security measures include, but are not limited to, usage of password systems, establishment of procedures to assure physical security of terminals, utilization of system usage audits, and update verification routines, and establishments of limits on the system usage capabilities given to terminals.

E. Auditing security measures on an annual basis shall be a part of the ongoing administration of the entity's computerized data system.

Emphasis shall be placed on the data security requirements of computerized files containing private or confidential data on individuals which are accessible directly via telecommunications technology, including security during transmission.

(R 359)

2 MCAR § 1.218 Administrative appeal. Pursuant to § 15.165, subd. 4 of the Act, an individual may appeal an adverse determination of a Responsible Authority to the Commissioner of Administration.

A. The appeal shall follow the procedures established in Minn. Stat. ch. 15, as amended, and the rules of the Office of Hearing Examiners relating to Contested Case Proceedings.

B. Notice of an appeal must be submitted to the Commissioner of Administration within a reasonable time of the determination made by the Responsible Authority pursuant to § 15.165, subd. 4 of the Act.

1. The notice shall be in writing and addressed to the Commissioner of Administration, State of Minnesota, 50 Sherburne Avenue, St. Paul, Minnesota 55155.

2. The notice shall contain the following information:

a. The name, address, and phone number, if any, of the appealing party.

b. The name of the Responsible Authority and the entity which he or she represents.

c. A description of the nature of the dispute, including a description of the data.

d. A description of the desired result of the appeal.

3. The Commissioner of Administration may require additional information if it is reasonably necessary in order to establish the Contested Case Proceeding.

4. Upon written request of the data subject stating reasons, the appeal may be processed under the name of a pseudonym.

C. The Department of Administration shall be reimbursed for all costs associated with the Contested Case Proceeding by the entity whose Responsible Authority has been the impetus for the individual's appeal to the Commissioner of Administration.

1. The commissioner shall establish appropriate accounting procedures to provide to the entity an itemized invoice.

15.165

Subd. 4. An individual may contest the accuracy or completeness of public or private data concerning himself. 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: (a) 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 (b) notify the individual that he 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.

25

(R 359)

2 MCAR § 1.219 General powers of the Commissioner of Administration. Pursuant to § 15.163, subd. 2 of the Act and to assist in the general implementation and enforcement of the Act, the commissioner shall have the following powers:

A. If the commissioner determines that certain information is relevant to monitoring any entity's data collection and handling practices, policies and procedures, the commissioner shall require the Responsible Authority of such entity to submit the information.

B. Any inquiries concerning the Act or these rules and any information submissions required to be made by subd. A. of this rule shall be directed to the Data Privacy Unit, Department of Administration, State of Minnesota, 50 Sherburne Avenue, St. Paul, Minnesota 55155.

C. The Data Privacy Unit shall respond promptly to all inquiries within personnel and budgetary limitations.

15.163 REPORTS TO THE LEGISLATURE.

Subdivision 1. On or before August 1, 1976, the responsible authority shall prepare a public document containing his 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 his state agency, statewide system, or political subdivision. 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 keep it accurate.

Subd. 2. 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.

(R 359 -360)

2 MCAR § 1.220 Duties of the Commissioner of Administration relating to emergency classification of Data. Pursuant to Minn. Stat. § 15.1642, the commissioner and Responsible Authorities shall comply with the following:

A. The Responsible Authority, pursuant to § 15.162, subd. 6 of the Act, shall prepare any application for emergency classification in writing in a form provided by the commissioner.

1. The form for an application is set out in the appendix to these rules. Copies of the form are available from the Data Privacy Unit.

B. For the purposes of the administration of § 15.1642 of the Act, the following terms have the meanings given to them:

1. "Days" means calendar, not working days.

2. "Upon filing" means upon receipt of either an original or amended application by the commissioner.

3. "Date of disapproval" means the date the Responsible Authority actually receives the disapproval notification from the commissioner.

4. "Within 20 days of submission to the Attorney General" means within 20 days of the date that the Attorney General's Office in the Department of Administration actually receives the record from the commissioner.

C. Application for emergency classification of data shall be submitted to the Data Privacy Unit, Department of Administration, State of Minnesota, St. Paul, Minnesota 55155.

D. If the Data Privacy Unit requires the Responsible Authority to submit additional information in support of the application, that application is deemed to have been filed on the date the additional material is received by the Data Privacy Unit. The commissioner shall return any application to the applicant if the additional information requested is not received within 30 days.

E. The provisions of this rule shall terminate and cease to have force and effect on whichever of the following dates or events occurs later:

1. On August 1, 1979; or

2. On the effective date of a statute that repeals the commissioner's authority to rule on emergency classification of data, pursuant to Minn. Stat. § 15.1642, subd. 3.

15.1642 EMERGENCY CLASSIFICATION.

Subdivision 1. APPLICATION. The responsible authority of a state agency, political subdivision or statewide system may apply to the commissioner for permission to classify data or types of data on individuals as private or confidential, for its own use and for the use of other similar agencies, political subdivisions or statewide systems on an emergency basis until a proposed statute can be acted upon by the legislature. The application for emergency classification is public.

Upon the filing of an application for emergency 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 30 days, or until the application is disapproved or granted by the commissioner, whichever is earlier.

Subd. 2. CONTENTS OF APPLICATION. An application for emergency classification shall include and the applicant shall have the burden of clearly establishing at least the following information:

(a) That no statute currently exists which either allows or forbids classification as private or confidential;

(b) That data similar to that for which the emergency classification is sought has been treated as either private or confidential by other state agencies or political subdivisions, and by the public; and

(c) That a compelling need exists for immediate emergency 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. The commissioner shall either grant or disapprove the application for emergency classification within 30 days after it is filed. If the commissioner disapproves the application, he shall set forth in detail his reasons for the disapproval, and shall include a statement of what classification he believes is appropriate for the data which is the subject of the application. Ten 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 on individuals, unless the responsible authority submits an amended application for emergency classification which requests the classification deemed appropriate by the commissioner in his 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 15 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 15 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 on individuals. No more than one amended application may be submitted for any single file or system which contains data on individuals.

If the commissioner grants an application for emergency 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 20 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 4. All applications for emergency classification which are pending on the effective date of this section shall be deemed to have been filed on the effective date of this section.

Subd. 5. EXPIRATION OF EMERGENCY CLASSIFICATION. All emergency classifications granted under this section and still in effect shall expire on July 31, ~~1978~~ 1979. No emergency classifications shall be granted after July 31, ~~1978~~ 1979.

STATE OF MINNESOTA
OFFICE OF HEARING EXAMINERS

FOR THE COMMISSIONER OF ADMINISTRATION

In the Matter of the Proposed Adoption of Rules of the Department of Administration Governing Enforcement and Administration of the "Minnesota Data Privacy Act." (2 MCAR §§ 1.201 - 1.220)

REPORT OF HEARING EXAMINER

The above-entitled matter came on for hearing on October 31, 1978, in St. Paul before Steve M. Mihalchick, Hearing Examiner assigned by the Chief Hearing Examiner.

This is a rules hearing pursuant to Minn. Stat. ch. 15, to determine whether proposed rules governing the enforcement and administration of the Minnesota Data Privacy Act should be adopted.

The following persons appeared for the Department of Administration: Daniel McGraw, Assistant Commissioner; Donald Gemberling, Manager of Data Privacy Unit; Sheila Fishman, Special Assistant Attorney General.

Eighty-eight persons attending the hearing signed the hearing register. The hearing continued until all interested persons and all interested groups had had an opportunity to be heard.

Pursuant to Minn. Stat. § 15.0412, subd. 4, this Report shall be available for review to all affected individuals upon request for at least five days. Thereafter, the Commissioner shall, if he proposes to adopt the rules as originally proposed or amended, submit a copy of the Order Adopting Rules, a copy of any additional agency findings, a copy of the rules as originally proposed, and a copy of the rules as adopted to the Chief Hearing Examiner for review pursuant to Minn. Stat. § 15.052, subd. 4. The submission to the Chief Hearing Examiner shall precede review by the Attorney General. The Chief Hearing Examiner shall complete his review and submit his report to the Commissioner on the issues of substantial changes in the rule and compliance with Minn. Stat. § 15.0412 within ten calendar days. The Commissioner will be responsible for filing the rules with the Attorney General and for notifying persons who have indicated that they wish to be notified of such filing.

Based upon the record herein, the Examiner makes the following:

FINDINGS OF FACT

PROCEDURAL REQUIREMENTS

1. On August 21, 1978, the Department filed the following documents with the Chief Hearing Examiner:

   (a) A copy of the proposed rules.
   (b) The Order for Hearing proposed to be issued.
   (c) The Notice of Hearing proposed to be issued.
   (d) A Statement of the number of persons expected to attend the hearing and estimated length of the Agency's presentation.

2. On September 4, 1978, a Notice of Hearing and a copy of the proposed rules were published at 3 State Register 346.

3. On September 14, 1978, the Department mailed the Notice of Hearing and proposed rules to all persons and associations who had registered their names with the Secretary of State for the purpose of receiving such notice and to all state agencies, political subdivisions, and other interested entities.

4. On October 5, 1978, the Department filed the following documents:

(a) The Order for Hearing.
(b) The Notice of Hearing as mailed.
(c) The Affidavit of Receipt of the Secretary of State's list.
(d) The Affidavit of Mailing the Notice to all persons on the Secretary of State's list and affected governmental agencies.
(e) The Secretary of State's Certificate and list.
(f) The Statement of Need and Reasonableness.
(g) All materials received following a Notice of Intent to Solicit Outside Opinion published at 2 State Register 2167 (6/5/1978)
(h) The names of Department personnel who will represent the Agency at the hearing together with the names of any other witnesses solicited by the Agency to appear on its behalf.
(i) An Affidavit of Review by the Intergovernmental Information Systems Advisory Council.

The documents were available for inspection at the Office of Hearing Examiners from the date of filing to the date of the hearing.

5. The record remained open through November 20, 1978, for the receipt of written comments and statements. Thirty-nine public comments were received following the hearing.

6. On December 20, 1978, the Department and Hearing Examiner requested that an extension be granted to the 30-day requirement for filing of the Examiner's Report. The extension was granted by the Chief Hearing Examiner.

7. Minn. Stat, § 15.1671, provides:

> The commissioner /of administration/ shall with the advice of the intergovernmental information services advisory council promulgate rules, in accordance with the rulemaking procedures in the administrative procedures act which shall apply to state agencies, statewide systems and political subdivisions to implement the enforcement and administration of sections 15.162 to 15.169. The rules shall not affect section 15.165, relating to rights of subjects of data, and section 15.169, relating to the powers and duties of the privacy study commission. 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 15.0412, subdivision 3, of the date and place of hearing, enclosing a copy of the rules and regulations to be adopted.

NEED AND REASONABLENESS OF THE PROPOSED RULES

8. Except as found below, the Examiner adopts the attached Statement of Need and Reasonableness as findings that the Department has demonstrated the need for and reasonableness of its proposed rules and that the proposed rules fulfill all substantive requirements of law and rule. As a number of persons stated, Mr. Gemberling has done an excellent job of developing comprehensive and fair rules to implement and enforce a complex and sometimes controversial Act. The rationale provided in the Statement of Need and Reasonableness is also comprehensive and well done.

2 MCAR § 1.201 - SCOPE AND PURPOSE

9. Section 1.201 A. simply states that the rules shall apply to those government entities defined in cited portions of the Data Privacy Act. This is necessary and reasonable for reasons stated in the Statement of Need and Reasonableness. The Department of Public Welfare proposed that the Statement should be expanded and, consequently, that the scope of the rules should be expanded, to include all agencies under contract to a state agency or political subdivision which, by the terms of their contract, subject themselves to all privacy laws and rules to which the agency or subdivision letting the contract is subject. DPW acknowledges that such a reference would go beyond the mandatory coverage of the privacy law which, by definition in Minn. Stat. § 15.162, subd. 5, includes social service agencies and non-profit corporations that handle data on individuals because of a contract with a state agency, political subdivision or statewide system. The Commissioner may wish to consider this addition to the rules though the Examiner would view it as not being necessary. If a contracting party wishes to bind itself by some law, it may generally do so.

10. Section 1.201 B. clarifies the application of the Act to non-profit social service agencies. The Minnesota Association of Community Mental Health Programs, Inc., commented that this subsection seemed vague (Pub. Ex. 39). This section is not vague at all, and perhaps what was really feared was the burden these rules would impose on purchase of service contracts by the political subdivisions. For example, the Ramsey County Commissioners were concerned about the massive effort that would be entailed in terms of requiring and monitoring compliance by these agencies (Pub. Ex. 18). As was pointed out many times at the hearing, most of the requirements imposed are done so by the Act and not by these rules. As should become more clear later, many of the burdens imposed by the rules are not as onerous as they first appeared.

The Minnesota Association of Health Care Facilities (MAHCF), in comments at the hearing, and in writing (Pub. Ex. 21), expressed its concern about whether non-proprietary nursing homes that contract with the State through written provider agreements to provide nursing care services to medical assistance recipients fall within the definition of non-profit social service agency. Mr. Gemberling expressed his opinion at the hearing that they would be included within the definition. MAHCF noted that nursing homes are not providing a traditionally "governmental" service which seems to be the type of agency intended to be covered by Minn. Stat. § 15.162, subd. 5. Further, the statute only applies to non-profit social service agencies, and thus, the statute would treat proprietary nursing homes differently from non-proprietary nursing homes, even though both types provide services to medical assistance recipients under contracts from the Department of Public Welfare. The Department should clarify the rule.

11. Section 1.201 D. provides:

> Nothing in these rules shall limit the discovery procedures available at law to any party in a civil or criminal action or administrative proceeding as described in the Minnesota

Rules of Civil Procedure and the Minnesota Rules of Criminal Procedure as adopted by the Supreme Court or in Minnesota Statutes.

The Examiner would note first of all that procedural rules of administrative proceedings are not described in the civil or criminal rules and would suggest that the final portion of the sentence should read:

". . . or in Minnesota Statutes and rules adopted thereunder."

The law firm of Holmes, Kircher & Graven attacked this provision rather strenuously. They note first that the Act itself does not create the exception and that the Act provides that private or confidential data on individuals shall not be used, collected, stored or disseminated for any purposes other than those stated to an individual at the time of collection. Thus, they argue, unless an individual is notified at the time of collection that data he or she discloses will be subject to discovery, the proposed rule is clearly in excess of the scope of the Act, and as such, is beyond the Commissioner's authority to adopt as a rule (Pub. Ex. 2). In summary, the firm states:

"If the courts choose to create an exception to the Act for the operation of their independent powers, that is for the courts to determine. But the Department, as the agency charged with the implementation and administration of the Act, should take the strongest and most protective position possible, creating no exceptions not provided for in the Act."

It is the interpretation of the Department that the Act was not intended to affect the operation of discovery procedures because the discovery rules are a fundamentally important provision essential to the workings of the judicial system. The Department's position is not unreasonable.

The Department of Public Welfare submitted a good comment on this subsection:

"The Department of Public Welfare operates many of its programs under regulations issued by the United States Department of Health, Education and Welfare. The most significant of these regulations as regards data privacy is 45 CFR 205.50. These regulations require that all agencies which receive federal monies for public assistance and social services must have in place, a state plan which protects the confidentiality of recipient information. The State Data Privacy Act and the proposed rule substantially put into effect for the welfare system in Minnesota all that is required by these federal regulations, with one exception dealing with how court orders may be issued for nonpublic information. /But see Finding No. 18/ Court orders and/or discovery are not precluded under the federal regulation guidelines, but they do require substantially that:

"In the event of the issuance of a subpoena for the case record or for any agency representative to testify concerning an applicant or recipient, the court's attention is called, through the proper channels, to the statutory provisions and the policies or rules and regulations against disclosure of information."

We would like to see similar language added to 2 MCAR 1.201 D which would require that:

"In the event of the issuance of a subpoena for any private or confidential information (to use the state language applicable to all agencies) or for any en-

good idea

> tity representative to testify concerning any individual on whom private or confidential data is maintained, the court's attention should be called, through the proper channels, to these statutory provisions, policies and/or rules and regulations against disclosure of such information."
>
> This language would not limit the court in its jurisdiction over the data, it would merely serve as a reminder to the court that there does exist, some limitations on disclosure which should be reviewed before any subpoena or search warrant is issued or before any individual is compelled to testify concerning private or confidential information. Such language would parallel the federal regulations and would bring to light alternatives such as in-camera review by the court prior to open court disclosure of private or confidential information. (Pub. Ex. 30)

The Examiner would suggest that language like that suggested by DPW should be added to this subsection. As suggested by Holmes, Kircher & Graven, there are sometimes alternative procedures available, and, as suggested by DPW, a provision such as this would help bring them to light. The Examiner would further suggest that whatever language is adopted by the Commissioner, it should include references to discovery orders as well as subpoenas and to administrative agencies as well as courts in order that it be consistent with the already proposed provisions of this subsection.

12. The comments by Holmes, Kircher & Graven in the previous subsection were also applied to section 1.201 E. which provides that the rules shall not restrict or limit the scope or operation of any judicial order or rule. In addition to its position taken in subsection D., the Department noted that the generalized operation of the Act should not take preeminence over the unique circumstances of a given case which has necessitated a judicial order.

13. The Minnesota Hospital Association was very concerned about the effect the rules would have upon the medical records maintained by approximately one-half of the hospitals in the state of Minnesota which are governmental entities of one sort or another and thereby subject to the Act. (Pub. Ex. 31) They request that a specific exclusion be included in § 1.201 of the rules stating that the rules shall not apply to medical records maintained by governmental entities. The Association argues that medical records are already protected by statutes and case law, that procedures already exist to protect the information adequately, and that the additional requirements imposed by the Data Privacy Act and the proposed rules would be extremely burdensome to these hospitals. The Association relies heavily on Minn. Stat. § 144.335 as a "more recent and more specific enactment than the Data Privacy Act /that/ deals very specifically with medical records." An examination of that statute shows, however, that it actually deals only with patient access to his own records and the discretion of the entity to refuse access if harm would result, but not at all with any of the other aspects of the Data Privacy Act or the proposed rules. The Act, itself, creates no exception for medical records and the Department's decision not to do so is not unreasonable.

14. The Dakota County Attorney also suggested the addition of a subsection to section 1.201 to read as follows:

"Compliance with these rules will relieve responsible authorities, their agents and/or employees from the sanctions imposed by Minn. Stat. § 15.166 and Minn. Stat. § 15.167 of the Data Privacy Act. (Pub. Ex. 31)

The writer apparently feels that there may be some liability exposure for noncompliance with the Act as a result of compliance with the rules. Since whatever rules are finally adopted are meant to clarify and make specific the Act, it is, technically, impossible for that result to occur. At any rate, the Commissioner has no authority to excuse violations of the Act. The Examiner does not recommend inclusion of this suggestion.

2 MCAR § 1.202 - DEFINITIONS

15. Section 1.202 B. defines arrest information to include only those elements of data listed in Minn. Stat. § 15.162, subd. 1a, in information that is collected by law enforcement agencies. The editors of the Minneapolis Star and the Minneapolis Tribune newspapers state that the first provision of the rule does nothing more than reference the statute and therefore is not needed. That is not quite true, because the statute does not explicitly exclude other elements. The rule thus clarifies the statute. Secondly, the editors object to the second portion of the definition defining arrest information in terms of who collects it. They feel the language of the statute is clear enough without further interpretation. Yet comments from the Department of Economic Security (Ex. 17) and the Department of Corrections (Pub. Ex. 29) indicate that there is indeed some confusion about the statutory definition of arrest information. For the reasons stated in the Statement of Need and Reasonableness, this definition is reasonable.

16. Section 1.202 C. defines "data" as a shorthand term for "data on individuals" as defined in the Act. Three provisions are added to make it clear that data on individuals is an all-encompassing term: (1) Data can be in any form; (2) the duration of the existence of the data is not relevant, and (3) all data is "data on individuals" if it can in any way identify a unique individual. The Mayor's office of St. Paul suggested that the last provision could be clarified by changing the term "a unique" to "any particular" (Pub. Ex. 33). This, and a number of the other grammatical suggestions made by the Mayor's office, should be adopted.

OK

Section 1.202 C.4. states that code numbers representing unique individuals constitute "data on individuals" if a list or index of any type is made available by which the individual can be identified. But, such data may qualify for treatment as summary data pursuant to 2 MCAR § 1.209. The Office of the Hennepin County Attorney (Pub. Ex. 26), and the Minnesota Association of Community Mental Health Programs, Inc. (Pub. Ex. 39) both expressed concern over the possible loss of confidentiality where code numbers were treated as summary data and therefore publicly available. Hennepin County expressed some confusion as to what the rule actually meant. The Examiner agrees that the section is confusing. If the underlying data is confidential or private, then, under § 1.202 M.2., it is not summary data if the list or index by which any individual can be identified is available to persons who gain access to or possession of the underlying

I agree

data. On the other hand, if that index or list is not available, then the underlying data would not be "data on individuals" under the definition here. This rule should be clarified.

17. Section 1.202 D., Confidential Data. This term is defined in terms of who can gain and who is denied access to the data and requires that a state statute or federal law "provide substantially" for certain treatment. Comments on this section dealt with the term "provides substantially", calling it vague. (Pub. Exs. 14 and 23) In its posthearing response to the Minnesota School Boards Association's comments on this issue (Pub. Ex. 14), the Department stated:

> The concern evidenced by MSBA's comments in the first paragraph under 2. and 3. seems to be with the "substantially provides" language in certain definitions and with the "discretion" of responsible authorities to classify data. It is clear from a reading of the statute that in actuality responsible authorities have little or no discretion in classifying data. Responsible authorities are required to make a determination based on a reading of Minnesota Statutes and federal law as to whether certain data under their custody is anything other than public. The sole purpose of the "substantially provides" language is to allow responsible authorities to make a proper reading of old state statutes and federal law where those references do not use the specialized definitions of the terms private, public and confidential that are in use in Minnesota.
>
> It is the opinion of the Department that "substantially provides" is not vague. The full text of the definitions provides the Responsible Authority with necessary guidance in evaluating authority to withhold data from the public as required by Minnesota law. We completely fail to see how use of this language makes these rules unreasonable as suggested by the MSBA comments. The assertion by MSBA that "substantially provides" is the only guidance provided to Responsible Authorities is not correct. Each of the definitions the MSBA comments identify contain substantial guidance, within the statutory limits. Again, it appears to us that MSBA's argument goes to the statute and not to the Rules. (Dept. Ex. O)

It might first be noted that "vagueness" is a constitutional due process concept most used to measure the validity of laws that described criminal conduct or infringe in some manner on First Amendment rights. Its application to administrative rulemaking is less stringent, but some rules have been held to be unreasonable because they were so unclear as to have little or no meaning. At any rate, the Examiner agrees with the Department that the use of the term "provides substantially" is not unclear and is, in fact, necessary and reasonable so that responsible authorities can properly apply state statutes and federal law as they are required to do by the Act.

The Ramsey County Commissioners felt that the definition was clear as to state statutes and federal law but remained vague as to court decisions. They suggested that it would be helpful if the proposed rules specifically addressed the general impact of state court decisions relating to the issue of data privacy (Pub. Ex. 18). The comment points out specifically the case of County of Sherburne v. Schoen, 306 Minn. 171, 236 N.W.2d 592 (1975), as a case that held certain data to be confidential. As far as state law is concerned, the Data Privacy Act, itself, allows data to be confidential or private only if so required by the state statute. Thus, the Department cannot broaden that definition to include case law or administrative regu-

lations. Further, in County of Sherburne v. Schoen, the Court actually interpreted the Data Privacy Act as it existed at that time and said that certain data was confidential under the Act. The effect of such cases is to assist responsible authorities in determining whether data they maintain is confidential, private or public.

18. Section 1.202 E. defines private data. There were a great number of comments about this subsection.

One major concern involves a situation where federal regulations may require that in order to receive federal monies, the state must provide some certain amount of privacy for data on individuals obtained under the program. These same federal regulations do not, however, themselves classify that data as private or confidential and thus, do not provide the legal authority for a responsible authority to do so. The comments of the Hennepin County Attorney (Pub. Ex. 26) state the problem well:

> 2 MCAR § 1.202 E.3.(as indicated on the erata (sic) sheet) stating that a federal agency rule requiring that political subdivisions provide for the confidentiality of data does not of itself make data private, poses serious problems for the welfare programs of the state. There are numerous federal regulations in this area requiring that the state system or political subdivision provide for the confidentiality of data obtained from data subjects. If this is not done, the potential exists for a violation of the Federal regulations resulting in serious penalty for the state or political subdivisions, including loss of federal participation in the funding of various programs. Thus, if the Legislature fails to provide for the confidentiality of this data, and if it is not provided for by emergency classification, the present regulations would seem to indicate that the data is public and could result in very costly consequences for the state and political subdivision, particularly in the welfare area.
>
> An example of this is the scheme required by the U. S. Department of Health, Education and Welfare under Titles IV-A, XIX and XX of the Social Security Act, which require that "state plans" comply with 45 CFR 205.50. This federal regulation requires each state to safeguard information obtained in the running of programs of aid to families with dependent children and medical assistance. We see no rational (sic) for Minnesota to oppose this federal requirement since it has been complied with for several years. In addition, compliance is a necessary condition in order to receive millions of dollars from the federal government.
>
> This office believes that the statute is ambiguous on the question of whether federal regulations of this type actually classify data. We believe, therefore, that the ambiguity could be clarified in either direction by the proposed regulations. We would, therefore, strongly urge that 2 MCAR § 1.202, E.3. be rewritten to provide substantially that federal rules of this kind do in and of themselves make the data referred to private.

Currently, the absence of a specific state statute classification is dealt with by the power granted to the Commissioner to grant emergency classifications under Minn. Stat. § 15.1642, but that system is only to be used ". . . until a proposed statute can be acted upon by the legislature." Further, the Commissioner's authority to grant emergency classifications will expire July 31, 1979. It would be contrary to the statute to attempt to implement Hennepin County Attorney's suggestion that federal rules

requiring state agencies to provide for the protection of data on individuals in and of themselves make that data private or confidential. By their own terms, they do not do so. Under the Act and those federal requirements, the governmental entities must seek legislation properly classifying the data they maintain before July 1, 1979. It is also possible to imagine some changes to the Act that would cure the problem.

19. A second major problem that applies to classification of data on individuals is that there exists under some statutes data that is sometimes private and sometimes confidential. That is, the subject of the data may or may not have access to it, depending on different factors. The most glaring example of this is pointed out by the Minnesota Hospital Association, again referring to medical records and Minn. Stat. § 144.335. The first two paragraphs of Minn. Stat. § 144.335, subd. 2, require health care providers to supply a patient's health record to him upon request. Assuming that some other state statute or federal law makes such health records non-public, this would mean that such data is private data. However, the third paragraph of that subdivision provides:

> If a provider, as defined in subdivision 1, clause (b)(1), reasonably determines that the information is detrimental to the physical or mental health of the patient, or is likely to cause the patient to harm himself or another, he may withhold the information from the patient. The information may be supplied to an appropriate third party or to another provider, as defined in subdivision 1, clause (b)(1). The provider or third party may release the information to the patient.

Thus, if the provider makes such a determination, the data becomes confidential data by operation of the statute. Logically, the way to handle such data is to call it confidential and handle it as confidential but release it to the patient except where a determination of harm is made.

The proposed rules deal with this situation in § 1.202 E.1.d. which provides the following example of private data:

> Data is private if a state statute or federal law provides substantially that:
>
> * * *
>
> d. Certain data shall be confidential and may be shown to the data subject at the discretion of the person holding the data. Such data shall be private if the state statute or federal law does not provide standards which limit the exercise of the discretion of the person maintaining the data.

(Due to a typographical error in the errata sheet submitted by the Department at the hearing (Dept's Ex. L), it appeared that this paragraph had been deleted from the proposed rules; that was not the Department's intent.) The implication of that paragraph is that if standards limiting the exercise of discretion do exist, the data is confidential data, but that is not very clear. Several comments requested that it be clarified (e.g., Pub. Exs. 8, 27 and 31) The Minnesota Hospital Association suggested specific language that could be used to clarify this issue. Its suggestion is as follows:

> The first alternative would be to further define confidential data so that 2 MCAR § 1.202 D. would read as follows:

Confidential Data as defined in § 15.162, subd. 2 of the Act, shall only include data which is expressly classified by either a state statute, including the provisions of § 15.1642 of the Act, or federal law.

1. Data is confidential only if a state statute or federal law provides substantially that:

   a. Certain data shall not be available either to the public or to the data subject; or
   b. Certain data shall not be available to anyone for any reason except agencies which need the data for agency purposes.
   c. Certain data shall be confidential if a a state statute or federal law provides that the data may be shown to the data subject only at the discretion of the person holding the data, and if such state statute or federal law provides standards which limit the exercise of the discretion of the person maintaining the data.

2. Data is not confidential if:

   a. A state statute or federal law provides that the data is confidential, but the context of the statute or federal law, in which the term confidential appears, reasonably indicates that data is accessible by the data subject, or if the data subject is given access to the data only upon the discretion of the person holding the data and the state statute or federal law does not provide any standards which limit the exercise of such discretion.

3. A state agency rule, an executive order, an administrative decision, or a local ordinance shall not classify data as "confidential," or use wording to make data inaccessible to the data subject unless there is a state statute or federal law as the basis for the classification.

The foregoing amendments would clarify that under certain circumstances, data which may sometimes be confidential can be considered as such within the formal classification system and still be accessible to the data subject upon the proper exercise of discretion by the person holding the data. In the case of medical records as access to those records is defined by Minn. Stat. § 144.335, this would be a compatible and workable method of classifying these records. In other words, the records would be classified "confidential/private," and access would depend on the different variables that have already been contemplated in the enactment of Minn. Stat. § 144.335.

The second amendment would be relative to 2 MCAR § 1.202 E. which should be amended to read as follows:

Private Data, as defined in § 15.162, subd. 5a of the Act shall only include data which is expressly classified by either a state statute, including the provisions of § 15.1642 of the Act or federal law.

1. Data is private if a state statute or federal law provides substantially that:

   a. Certain data shall not be available to the public but shall be available to the subject of the data;

b. Certain data shall not be available to anyone, except the data subject or his designated representative such as an attorney;
c. Certain data shall be confidential and the person the data is about may view the data at reasonable time; or
d. Certain data shall be ~~confidential and may be~~ shown to the data subject at the discretion of the person holding the data. ~~Such data shall be private if~~ , but the state statute or federal law does not provide standards which limit the exercise of the discretion of the person maintaining the data, in which case the data shall be private.
e. The data is confidential, but the context of the statute or federal law in which the term confidential appears, reasonably indicates the data is accessible by the data subject.

* * *

We would also urge changes in the substantive provisions, as distinguished from the definitional provisions which define the kinds of access that persons have to different types of data. Specifically, it is the recommendation of the Minnesota Hospital Association that 2 MCAR § 1.204 A be amended to read in relevant portion as follows:

A. Access to private data shall be available only to the following:

1. The subject of such data, limited only as provided in Minn. Stat. s 144.335.

Further amendment would be appropriate relative to 2 MCAR § 1.206 which could be amended to read in relevant portion as follows:

A. Access to confidential data is available only to the following:

1. Individuals within the entity, whose work assignments reasonably require access.
2. Entities and agencies who are authorized by statute, including § 15.1641 of the Act, or federal law to gain access to that specific data.
3. Individuals to whom access to otherwise confidential data has been authorized by the responsible authority under the provisions of Minn. Stat. § 144.335.

The combination of these various amendments would, we believe, allow the type of flexibility that is absolutely essential in properly serving the public in terms of appropriate handling of medical records. (Pub. Ex. 27)

The Examiner recommends that the changes or additions suggested for §§ 1.202 D.1.c., 1.202 D.2.a. and 1.202 E.1.d. except the last proviso, should be adopted for the reasons given by the Association. Their other suggestions seem unnecessary and could be confusing. Finally, the suggested addition to § 1.206 A.3. should not be limited to Minn. Stat. § 144.335. There are no doubt other state statutes and federal laws that create this shifting type of non-public data on individuals, so more general language should be used.

20. The Hennepin County Chiefs of Police Association and the Minnesota Police Chiefs Association have both passed a resolution recommending

legislation to classify certain criminal justice information as confidential and private. (Pub. Exs. 7 and 13) The resolution recognizes that classification must be done by statute and not by these rules.

21. Section 1.202 F. defines public data on individuals. The Department testified that the confusion and controversy surrounding the meaning of public data has been the main stumbling block to implementation of the Act over the past few years. Minn. Stat. § 15.162, subd. 3, states: "Data on individuals are classified as public, private or confidential." Under Minn. Stat. § 15.162, subd. 5b, "Public data on individuals" means "Data which is accessible to the public in accordance with the provisions of section 15.17." Whether records are "public records" under Minn. Stat. § 15.17, subd. 1, depends on whether they are "necessary to a full and accurate knowledge" of official activities. Kottschade v. Lundberg, 280 Minn. 501, 160 N.W. 2d 135 (1968), Minnesota Medical Association v. State of Minnesota, ___ Minn. ____, ___ N.W. 2d ___ (November 24, 1978) The Kottschade case placed some "reasonable limits" on the statutory language when it determined that the legislature did not intend anything so sweeping as to require that "public record" include "any casual jotting, any tear-sheet observation, which discloses the promptings of official action. . . . " The Court imposed the reasonable limits by defining "official activities" to be limited to "official actions" as distinguished from "thought processes." Thus, there may be records kept by political subdivisions which relate to the processes by which decisions are reached but which are not required to be kept of record as information pertaining to an official decision. They therefore, are not accessible to the public under Minn. Stat. §. 15.17 and interpreted by Kottschade.

Stating that it is vital for the definition of public data on individuals to be as clear as possible, the Department proposes a rule that says data is public if (1) a statute or federal law says it must be available to the public; (2) a statute or federal law requires the data to be collected and does not classify it private or confidential; and (3):

> c. A state agency, statewide system, or political subdivision, without any express enabling authority to do so, collects certain data because that data is necessary to its operations; as defined in 2 MCAR § 1.216 B.1.

In § 1.216 B.1., the term "necessary" has a specialized meaning. At the hearing, Mr. Gemberling testified that he intended "necessary" as used in this section to have its normal meaning; that is, if governmental personnel feel that certain data is necessary to the operation of governmental agencies and programs, access to that information is equally necessary to anyone trying to understand that agency or program. If that is the Department's intention, then, at the least, the reference to § 1.216 B.1. should be deleted from this rule.

A number of comments noted that the proposed rules attempt to adopt and expand the Kottschade reasoning still left the definition of public data unclear (Pub. Exs. 14, 16, 20, 31 and 33) The comments of the Dakota County Attorney state the problem well:

> Our second comment concerns the definition of public data under 2 MCAR § 1.202, Subsection F. This subsection presents serious problems. Many of these problems were pointed out at the hearing but for the sake of emphasis some

of these problems will be set forth here. The primary problem regarding public data is the attempt under the proposed rules to define public under the standards set forth in Kottschade v. Lundberg, 280 Minn. 501, 160 N.W. 2d 135 (1968), without taking into consideration the exceptions set forth in this case. The difficulty here is that the Kottschade case labeled certain data which is collected by public officials as not being public data. In effect, the Kottschade case determined that there was an exception to the public data statute (Minn. Stat. § 15.17). The problem arises from the fact that the same data which was stated not to be public under the Kottschade case is not defined as being private or confidential by any state statute or federal law. The proposed rules make no attempt to classify such data and hence, there is a "gap" which exists between the definitions of data which are set out in the Data Privacy Act and in the proposed rules. It is vital to clear up the confusion found under the rules defining public data, because subsequent rules (i.e. 2 MCAR 1.210, 1.215, and 1.216) direct the Responsible Authority to identify all data and freely disseminate data defined as public. In addition, Minn. Stat. § 15.166 states that a Responsible Authority who violates any provision of the Act itself is liable to a person who suffers any damage as a result of the violation. The wilful violation of any provision of the Act constitutes a misdemeanor under Minn. Stat. § 15.167.

Our suggestion to this problem is defining public data under 2 MCAR § 1.202, subs. F as follows: "Public data is all data which is not classified by state statute or federal law as private or confidential data." This would eliminate the confusion created by the Kottschade case. At the Hearing held on October 31, 1978, the Department of Administration expressed its belief that Minn. Stat. § 15.162, Subd. 3 (which provides in part that: "Data on individuals are classified as public, private or confidential") gives them the rule making power to come to such a determination, i.e. that all data which is not private or confidential is public. If you believe this to be the case, 2 MCAR § 1.202, Subs. F should be amended as described above in your report. If not, it is our suggestion the promulgation of these rules be delayed until such time as the legislature has had a chance to take further action delineating exactly what public data includes in light of the Kotschade (sic) case.

As presently proposed, the rule fails to meet substantive requirements of law that persons affected by or required to perform some act by a rule must be able to reasonably understand the rule. The Department noted the great need to make "public data" clear, but by this rule, has not done so. It is still unclear to those governmental entities that must operate under it. The Examiner would recommend that the rule could be made reasonable by adopting Dakota County Attorney's suggestion that if data on individuals is not classified private or confidential by proper authority, it is public data on individuals. As pointed out by counsel for the League of Minnesota Cities at the hearing, that is probably what the proposed rule says now, especially in light of §§ 1.202 D.3. and 1.202 E.3., which prohibit governmental entities from classifying data on individuals as confidential and private without appropriate authority to do so. In its posthearing comments, the Department stated that it had the following dilemmas in dealing with public data:

5.a. If the so-called "gap" theory is a viable theory of statutory construction, then assessor's field cards are not official records within the meaning of Minn. Stat., Section 15.17 and therefore they are not accessible to the public. However, as we pointed out

at the hearing, we are faced with the following dilemmas in dealing with publid data:

(a) The Kottschade case is ten years old and was decided on very narrow grounds.

(b) The intervening ten years has seen an explosion in the concepts of freedom of information and openness in government.

(c) Although the subject of Minn. Stat. 15.17 is official records, the subject of the privacy act is all data on individuals maintained by the state and its political subdivisions.

(d) The last sentence of Minn. Stat., Section 15.162, Subdivision 3 states very clearly: "Data on individuals are classified as public, private or confidential."

(e) Over and over public administrators have told us they cannot implement the privacy law because they cannot establish, given the definitions of public data in the statute, what data is public within their agencies.

The Examiner agrees with the Department that it has the authority to define public data on individuals as that which is neither private nor confidential. As Mr. Gemberling pointed out at one point in the hearing, by § 15.162, subd. 3. the Legislature, at least as to data on individuals, said that there were only three types of data. The problem is created by Minn. Stat. § 15.162, subd. 5b which states, "Public data on individuals means data which is accessible to the public in accordance with the provisions of section 15.17." The Examiner would suggest that it is not appropriate to use that subdivision to determine whether certain data on individuals is public, because that determination is to be made by elimination under section 15.162, subd. 3. Rather, subdivision 5b should be read to mean that the accessibility methods and procedures of section 15.17, subd. 4, must be applied to all public data on individuals. The "Gap" should only apply to records that do not contain any form of data on individuals.

It must be noted that some of the public comments did not support the concept of defining all data on the individuals that was neither confidential nor private as public. The Office of the Mayor of St. Paul suggested that it needed the fourth non-public records category found under the Kottschade theory ". . . to protect the individual from public disclosure of the information which would constitute an invasion of personal privacy." (Pub. Ex. 33) They stated that if the fourth category is eliminated ". . . the State of Minnesota and its governmental subdivisions will be faced with an election to either destroy, and in the future not record, much of the data necessary to its operation or to risk grave and substantial abuses of the individual liberties of its citizens."

22. Minn. Stat. § 15.162, subd. 8, provides:

"Statewide system" includes any record-keeping system in which data on individuals 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.

According to the Statement of Need and Reasonableness, although the term is defined by the Act, a clearer statement of the definition is necessary to assure that all statewide systems are indeed regulated. Section 1.202 H.3. of the proposed rules provides:

> 3. Statewide systems shall include, but are not limited to, recordkeeping and data administering systems established by statute, federal law, administrative decision or agreement, or joint powers agreement.
>
> a. Statewide systems shall include, but are not limited to, the Criminal Justice Information System administered by the Bureau of Criminal Apprehension, the Statewide Accounting System, the Minnesota Education Computing Consortium, and the various welfare systems primarily administered by the Department of Public Welfare.

This provision was the subject of a comment from the Minnesota School Districts Data Processing Joint Board, also known as TIES. This organization provides data processing services to each of the school member districts acting at the direction of each district. TIES does not collect initial information nor does it make decisions concerning the use of the information. These functions are performed by the individual school districts. The MECC referred to in the rule is a state entity formed by joint powers agreement which serves primarily to coordinate the data processing systems used by educational entities in Minnesota. The comment states:

> We do not know whether it was the intent of the Department to make all school district information systems part of a "statewide system" and thus remove from each school district the responsibilities pertaining to collection and use of data. If this was the intent, it would be a very far-reaching step which has no rational basis and no statutory basis, and which was neither explained nor justified in the Department's Statement of Need and Reasonableness. If this was not the intent, the draft should be clarified. It should provide only that whatever information is collected initially by MECC itself is a statewide system, and not that all school district data become part of a statewide system, merely because of the limited functions performed by MECC. (Pub. Ex. 34)

It would appear that TIES and MECC squarely fall within the proposed rule's examples because TIES is a record-keeping and data administering system established by joint powers agreement and the MECC is expressly named in the rule. However, it does not follow that such inclusion would . . . "Thus remove from each school district responsibilities pertaining to collection and use of data." It seems quite logical that confidential and private data must be protected under the provisions of the Act no matter where the governmental entities store that data or whom they have process it. On the other hand, it is not so clear whether the protection of that data requires the appointment of a responsible authority at the data processing center or whether the responsible authority, in this case, at the school district is adequate. It would seem that the latter would be adequate but the Examiner makes no specific recommendation on this comment.

23. Under the Act and these rules, data may be classified as confidential or private only by state statute or by federal law. Section 1.202 I. defines federal law because it is not defined by the Act. It provides:

> Federal law means United States Code, rules of Federal agencies as published in the Federal Register, and Federal case law including decisions of any court in the Federal judicial system.

The Office of the Hennepin County Attorney noted that the official compilation of the Federal rules, however, is in the Code of Federal Regulations and suggested that the Code of Federal Regulations be substituted for the Federal Register. The Department may wish to consider that change but the Examiner would caution that both the Federal Register and the Code of Federal Regulations publish items such as Federal guidelines which do not have the force and effect of law.

The Minnesota School Boards Association stated that by the definition of federal law, ". . . an extreme and unfair burden had been placed upon each responsible authority, that person's delegatees, and in the instance of school districts, the respective governing boards. It is unrealistic and impossible to expect each entity to be aware of all Federal agency rules and Federal case law." (Pub. Ex. 14) In fact, the Act provides that it is the responsible authorities who must classify the data and so they must know the law. The rule provides some assistance by telling them where they can look for the federal law. It is also apparent that each type of political subdivision should be more aware of the law that affects it than anyone else. In other words, school districts should be more aware of federal laws affecting pupil records, for example, than the Department of Administration. If they aren't, the MSBA is not doing its job.

24. Section 1.202 L. clarifies some of the confusion caused by the Act's definition of responsible authority. The rule lists who shall be the responsible authority in a number of situations. The Department of Veterans Affairs points out that Minn. Stat. § 197.603, subd. 2, makes the county veterans service officer the responsible authority with respect to all records in his custody and that this would pre-empt the statement in the rule that county boards appoint the responsible authority. Veterans Affairs suggests that "Unless otherwise provided by state law," type language be inserted within the rule. Such language already appears in Minn. Stat. § 15.162, subd. 6, but the Examiner would recommend that it be restated within this rule to avoid any possible confusion.

The law firm of Holmes, Kircher & Graven, cited an instance in which the Department returned an emergency classification application of the St. Paul Housing and Redevelopment Authority because the City of St. Paul had appointed the City Clerk as responsible authority. The Department did not wish to grant a classification for only that portion of the City's records administered by the Housing Authority. The law firm pointed out that under Minn. Stat. § 15.162, subds. 5 and 6, Housing and Redevelopment Authorities are political subdivisions and thus may appoint responsible authorities. They state that the conflict between the Act and the Department's policies is not resolved by the proposed rules and should be clarified. It appears to the Examiner that there are two separate questions involved here. First, who shall be the responsible authority in the various forms of governmental entities? That is addressed by the rule. The

question raised by the law firm deals with the Department's reasons for denying an emergency classification when one political subdivision is created by or a part of another political subdivision. That is not addressed by the rule. The Department should determine whether such relationships change any of the duties and requirements specified in these rules and, if necessary, clarify the rule.

Counsel for the League of Minnesota Cities pointed out that the rule requires cities (and all other political subdivisions) to appoint individuals who are employees. In some instances, they may want to appoint some other official; for example, a City Clerk who may not technically be an employee. The rule is not unreasonable, but the Department may wish to modify it.

25. Section 1.202 M. defines "Summary Data". The term is defined in the Act, but because of questions that have been raised, the rule provides an expanded definition and gives examples.

The editors of the Minneapolis Star and the Minneapolis Tribune criticized this rule because ". . . it does not recognize the responsible authority's statutory duty to permit a person outside the agency to prepare the summary data if the person agrees in writing not to disclose the private or confidential data from which the summary data is prepared." (Pub Ex. 23) The rule is reasonable as proposed. It says what summary data is, not who prepares it. The latter subject is dealt with in section 1.209.

2 MCAR § 1.203 - ACCESS TO PUBLIC DATA

26. The editors of the Minneapolis Star and Minneapolis Tribune argued that the Commissioner has no authority to adopt this section. They stated:

> Sec. 1.203: This entire section is objectionable because it exceeds the scope of authority granted the Commissioner of Administration. Minn. Stat. 15.1671 empowers the Commissioner to "promulgate rules . . . to implement the enforcement and administration of sections 15.162 through 15.169." Although these sections deal with the collection, storage, and accuracy of public data, they do not address the dissemination of private and confidential data to third parties. See especially 15.1641 and 15.165. The issue of general public access to public data is addressed in Minn. Stat. 15.17, which is outside the scope of rule-making authority granted by Minn. Stat. 15.1671. (Pub. Ex. 23)

The Department replied specifically to this comment:

> We fail to understand the comment's assertion that the rule has some effect on "third parties". It is clear under the proposed rule that public data is accessible to anyone. As we stated at the public hearing, we are aware of the problems associated with the rule's dealing with public data. However, we fail to see how we can comply with the statutory requirement of Minn. Stat. Section 15.1671 without addressing the subject of public data. Without a clear understanding of what public data is, agencies will never be able to implement the privacy act. (Department's Ex. N)

The editors of the Minneapolis newspapers are correct that the proposed rule goes beyond the scope of the Commissioner's rulemaking authority because it deals with the dissemination of data to the public and attempts to implement the provisions of Minn. Stat. § 15.17, subd. 4. The Minnesota Medical Association case is controlling on this issue. In that case, the

Court held that certain records were necessary to the full and accurate knowledge of the Department of Public Welfare's official activities; were, therefore, public records accessible to the public under Minn. Stat. Sec. 15.17; and that the information contained in such records was "public data on individuals" under Minn. Stat. Sec. 15.162, subd. 5b. An issue was raised as to the effect of lack of rules to implement the Act. The majority opinion stated in part:

> Minn. St. 15.1621 requires the commissioner of administration to adopt, in accordance with the Administrative Procedures Act, rules "to implement the enforcement and administration of sections 15.162 to 15.169." The commissioner has not done so. Nevertheless, this failure cannot affect public access to "public" information. Nothing in sections 15.162 to 15.169 purports to govern dissemination of public data. Dissemination is governed by Minn. St. 15.17 to 15.174. Minn. St. 15.171 expressly authorizes the use of "alternative methods for the compilation, maintenance and storage of information contained in /official/ records" and provides that such methods must provide for access to the information "by those authorized by law to have access." Since the information sought here is public information, the Catholic Bulletin is authorized to have access to it. Its access is thus determined under the Official Records Act, and the commissioner's failure to promulgate rules under the Data Privacy Act is immaterial. See, Reyburn v. Minnesota State Board of Optometry, 247 Minn. 520, 527, 78 N.W. 2d 351, 1356 (1956).

The Examiner finds, therefore, that the Department has failed to demonstrate its statutory authority to adopt Section 1.203 as proposed. If the Department desires to address the subject of access to public data, the rule could simply state:

> "The responsible authority shall provide access to public data in the manner provided in Minn. Stat. Sec. 15.17, subd. 4."

The following findings regarding Section 1.203 are made for the sake of completeness recognizing that the Department may disagree with this finding of lack of authority.

27. With a few minor exceptions, the need for and reasonableness of this rule was generally supported by most interested persons. Such support was expressed at the hearing by counsel for the League of Minnesota Cities and counsel for the Minnesota Newspaper Association. The Newspaper Association especially supported the provision in Section 1.203 A. that access must be provided to any person regardless of that person's interest in the data. This, as explained in the Statement of Need and reasonableness is in accordance with the "modern" principles of access to government records. That not all persons agree with such principles was perhaps made most clear by comments from the city manager of Brooklyn Center who suggested that it should be within his authority to draw the fine line between the public's right to know and a person's right to privacy. (Pub. Ex. 28) For example, he would make certain records not available to salespersons but would make them available to individual citizens wishing to buy a certain piece of property. As the majority of the Court pointed out in Minnesota Medical Association, supra, the power to restrict public access to information has been retained exclusively by the legislature:

> The legislature has provided mechanisms by which the public may be denied access to information controlled by state agencies. It has further determined that public records are

to be available to the public "except as otherwise expressly provided by law." Minn. St. 15.17, subd. 4. These provisions evidence a legislative intent to retain full control of public access to information. The power to restrict access is given to administrative agencies only in emergency situations, and even that power is subject to legislative action. No power to restrict access is granted to the courts.

The provisions of Section 1.203 A. are necessary and reasonable.

28. Section 1.203 A.1. requires the responsible authority to establish procedures to describe how access may be gained. This is a very general requirement that does not require such procedures to be in writing. Such procedures may, under the provisions of the rule, limit the time of public access to normal office hours. The procedures must require the responsible authority to respond to a request for access within a "reasonable" time.

The Minnesota Newspaper Association and the Minnesota School Boards Association requested some further definition of the word "reasonable". Time limits and number of days have been considered by the Legislature in reviewing amendments to Minn. Stat. § 15.17. One reason such limits were not adopted was that no consensus or compromise emerged as to what the number of days should be. Given the broad range of data covered by the Official Records Act, including data which may be up to 50 years old and maintained in warehouse-type facilities, no better standard can be given than "reasonable time". (Department's Ex. O)

The Higher Education Coordinating Board suggested that the technical requirements for access procedures in this rule and following similar rules would cause great expense, especially since state agencies would be required to adopt such procedures through the rulemaking process. (Pub. Ex. 38) Assuming that the HECB is correct that formal rulemaking would be required, the requirements imposed are minimal and are necessary to implement the Act.

29. Section 1.203 A.1.c. requires the responsible authority to charge a reasonable fee for providing copies of public data unless the entities' costs are minimal. Section 1.203 A.1.d. lists five factors to be considered in determining reasonable fees. Support was expressed for permitting a reasonable fee to be charged (Pub. Exs. 12, 28 and 31), but clarification was requested to reconcile the requirement of the proposed rule with the statutory prohibition against most state agencies collecting any type of fee except as specified by law. (Pub. Exs. 9 and 11) Other comments suggested simply that charging a fee should be permissive with the entity providing the data. (Pub. Exs. 18 and 32) It was also suggested that in determining a reasonable fee, the cost of labor should include the cost of research and files as well as simply preparing the copies.

The Examiner finds that the requirement to charge a fee for providing copies is unreasonable because some agencies are prohibited by statute from doing so and because it is a matter of judgment that should be left up to the responsible authority. Further, the Department relied on the provisions of Minn. Stat. Sec. 15.17, subd. 4, in proposing this particular rule. That subdivision permits copying of public records at reasonable

times and further provides:

> . . . Upon the demand of any person, /the custodian of public records shall/ furnish certified copies thereof on payment in advance of fees not to exceed the fees prescribed by law."

Whether or not that language requires the custodian to charge a fee is not clear, but at any rate, it is clearly limited to certified copies and whatever the fee is may not exceed any fee that is set by law. The proposed rule would be reasonable if the word "shall" were changed to "may".

2 MCAR § 1.204 - ACCESS TO PRIVATE DATA

30. Section 1.204 A. lists the persons to whom access to private data shall be available. In addition to the subjects of the data and individuals within the entity whose work requires access, the rule lists entities and agencies who are authorized access to that specific data by appropriate law and entities or individuals given access by ". . . the express written direction of the data subject."

Two state agencies raised questions as to access to private data by agencies that exchange information with other agencies (Pub. Exs. 17 and 29). These agencies are apparently asking whether certain types of access are authorized by appropriate law. They should talk to Mr. Gemberling directly.

The editors of the Minneapolis papers objected to the requirement for written direction (Pub. Ex. 23). They state:

> Minn. Stat. 15.1641(C)(3) permits disclosure of private or confidential data on individuals if the data subject gives "informed consent." The proposed rule does not necessarily guarantee that consent will be "informed." Nor is there any statutory authorization for the limitation that the informed consent must be expressed in writing.

In its Statement of Need and Reasonableness, the Department stated that this provision reinforces an underlying rationale of the Act that data subjects retain some control over the data they provide to the government. In response to the editors' comment, the Department stated:

> The comment makes reference to "informed consent" as the authority for an individual to have an agency disseminate data about him or her. This comment reflects a misreading of the act. "Informed consent" only comes into play when the agency seeks to initiate a new purpose or make a new use of private or confidential data previously collected from a data subject. (See Minn. Stat. 15.1641 (c)). The rule deals with assuming the individual's ability to direct the dissemination of private data about himself or herself. Problems with this situation are common. They arise from the act, but are not expressly handled by the statute. (Depts. Ex. N)

Describing to whom access is granted is clearly a part of implementing the Act and is, therefore, within the statutory authority of the Department. Just as clearly, requiring authorization to be in writing is not unreasonable.

31. Section 1.204 B. requires responsible authorities to establish written procedures to assure that access is gained only by those parties identified in Section 1.204 A. and requires that those procedures include reasonable measures that will assure that the person seeking access is actually the subject of the data or his authorized representative. The proposed rule then goes on to state:

2. Such reasonable measures include, but are not limited to, the following:

a. Requiring the person seeking to gain access to appear at the offices of the entity to gain such access or requiring the notarized signature of any data subject who is unable to appear at the offices of the entity.

b. Requiring the person to provide reasonable identification.

Only the Dakota County Attorney supported the requirement for a notarized signature stating that, "Although realistically, the requirement of a notarized signature may not greatly eliminate false requests, such a requirement does serve to protect the responsible authority from liability exposure. . . ." (Pub. Ex. 31) Otherwise, there was uniform opposition to the requirement (Pub. Exs. 23, 24, 25, 27, 30, 32, 38 and 39). Insurance companies and hospitals stated that the requirement would unduly increase insurance costs and inject administrative delay in the claim process with no real increase in security of the data (Pub. Exs. 24 and 27) The Ramsey County Welfare Department stated that the requirement would impose a potential hardship on welfare clients that may not have funds for or access to a notary (Pub. Ex. 25). The editors of the Minneapolis papers put it another way: "Requiring a notarized signature is not the only way — nor always the best way — to carry out the intent of the statute." (Ex. 23) They then suggest that the introductory line of this paragraph should read:

"Examples of such reasonable measures include, but are not limited to, the following:"

The Examiner finds the requirement for notarized signatures, to the extent that it is an absolute requirement, to be unreasonable because of the burdens and costs it would impose without any practical benefit to the security of private data. The word "notarized" should be deleted from the rule.

The comment of the editors that the rule should be modified to state that it is listing merely examples may, in fact, be what was intended in the first instance. The language as originally proposed is unclear but it does not say that "such reasonable meausres must include . . . ." Unless the rule is clarified one way or the other, the rule fails to fulfill substantive requirements of law because it is unclear. If the Department chooses to call these items examples, then the requirement of a notarized signature is not unreasonable because responsible authorities are given the option of determining whether such a procedure would be reasonable in their given set of circumstances. Nonetheless, the Examiner would still suggest that the requirement not even be made an example.

32. The editors of the Minneapolis papers also suggested that a third example of a reasonable measure be added as follows: Determining through personal knowledge that the person authorizing release is the data subject." The Department may add more examples to its list should it believe them to be necessary.

33. Section 1.204 E. requires the responsible authority to charge the subject a reasonable fee for providing copies of private data. Unlike the parallel rule in the section on access to public data, Section 1.203,

the requirement here is based on a requirement in the Data Privacy Act, namely, Minn. Stat. Sec. 15.165, subd. 3, and so there is authority in the Department to impose the requirement. It should also be noted that if the Department deletes the rule regarding access to public data, it will be necessary to restate the factors used to determine a reasonable fee within this rule and to change subsequent references to Section 1.203.

2 MCAR Sec. 1.205 - ACCESS TO PRIVATE DATA CONCERNING DATA SUBJECTS WHO ARE MINORS

34. Under Minn. Stat. Sec. 15.162, subd. 4, parents, guardians or persons acting in their place have access to private data concerning their children, ". . . . 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 interests of the minor."

This rule implements that provision of the statute. The Minnesota School Boards Association stated:

> 2 MCAR 1.205 B.2.a. establishes a presumption that the parents have the authority to access the data unless the responsible authority is provided with evidence that there is a state law, court order or legally binding instrument providing to the contrary. Thus, in the case of a divorce or custody situation, either parent should be granted access unless the other has produced an order, etc. that denies it. The responsible authority does not appear to have to seek out this information. The burden in this instance does not appear to be on the responsible authority or on the parent seeking access but rather is on the parent seeking to deny access. This paragraph, however, provides less than complete protection to the responsible authority. It should state that the "responsible authority shall provide data to parents unless . . . ." (Pub. Ex. 14)

It is difficult to see how the MSBA suggestion would clarify anything or provide any greater protection to the responsible authorities. Further, as was pointed out by the Department in its posthearing comments (Dept. Ex. O), this particular rule was taken verbatim from the HEW rules implementing the Family Educational Rights and Privacy Act of 1974 (FERPA), which rule was adopted by HEW at the urging of educators.

35. Section 1.205 C. requires responsible authorities to establish procedures to provide access by the parents of a minor data subject and imposes certain requirements that must be contained in those procedures.

Section 1.205 C.1. allows the responsible authority to require that requests by minors to deny access to parents or guardians be in writing. The Office of the Mayor of St. Paul addressed one area which they thought was unclear (Pub. Ex. 33). They noted that no mention was made of the possibility that the child may not know of his parents' request for access to the data. They wondered whether the rules required the child to be informed of each request or not. They requested that it be clarified either way. At the hearing, clarification was requested regarding procedures to be used where a person has been adjudicated mentally incompetent and the Commissioner of Public Welfare has been appointed guardian. As the Department stated in its Statement of Need, this particular exception has raised many questions, especially from educators and social service

agencies, and the proposed rule attempts to answer those questions. The rule is not unreasonable as proposed, but the Examiner would recommend that the Department attempt to clarify these questions, too.

36. Section 1.205 C.2. lists factors by which responsible authorities should be guided in making a determination of whether to honor a request by a minor to deny parental access; tests by which to determine ". . . that withholding the data would be in the best interests of the minor," as required by the statute. The MSBA complained that the determinations to be made on the factors listed might be beyond the skill and training of the responsible authority, and that they might have to be referred to doctors, lawyers, social workers or a psychologist. The section of the Act cited above clearly requires the responsible authority to make the determination The factors listed are helpful, but nothing prevents the responsible authority from consulting an appropriate professional for advice.

37. Section 1.205 C.2.a.(6) was added to the proposed rules during the drafting stage at the urging of various public bodies. It states that the responsible authority should consider:

> Whether the data concerns medical, dental or other health services provided pursuant to Minn. Stat. §§ 144.341 through 144.347. If so, the data may be released only if failure to inform the parent would seriously jeopardize the health of the minor.

Two agencies requested that "other health services" be defined (Pub. Exs. 25 and 39). It appears to the Examiner that that would be beyond the Department's authority because the cited sections of the statutes are not within the scope of the Commissioner's rulemaking authority and these rules can do no more than refer to them.

Comments raised the issue of denying parental access at the responsible authority's discretion, even when not so requested by the minor, if disclosure to the parents could cause harm to the minor. The Minnesota Hospital Association stated:

> First, we wish to make it clear we understand that Minn. Stat. § 15.162, subd. 4, as well as Minn. Stat. § 144.335 provides that parents are in the same position, and have the same legal rights, as their minor children, except that Minn. Stat. § 15.162, subd. 4, provides an exception where the minors register an objection to the release of records. It is acknowledged that this presents difficult questions in terms of parent/child relationships, but it is a matter of state law and these rules may not countermand such a legislative pronouncement.
>
> However, in an apparent effort to countermand the statutory provision, the rules provide in an explicit statement that the responsible authority may deny access to private data when the minor requests that access by (sic) denied. Conversely, absent such an express request, the responsible authority could not deny access to the parents.
>
> We strongly object to the very narrow approach taken regarding this matter. As indicated above, it is contrary to Minn. Stat. § 144.335, which vests discretion in the health care provider. It runs contrary to the spirit of the statutes dealing with child abuse and indeed presents a very serious threat in the context of child abuse cases. Specifically, it is well-known that in many instances of child abuse (and we emphasize that this is a life threatening problem) advance notice to parents

that child abuse is suspected will immediately precipitate the removal of the child from the health care facility, even before a child in jeopardy can be taken into protective custody. Our primary concern is that the child himself is required to initiate the request for withholding information. This does not adequately serve a young victim of child abuse, for example, who neither understands that access may be denied nor is capable of making such a decision. To compound this, a written request may be required. Again, the child who is too young to write or who is intimidated by a writing is not protected. If the physician makes his own decision to withhold information from the parents, it is unclear as to what his potential liability may be.

Carrying forward with 2 MCAR § 1.205 C.1. as proposed, especially if the rules are extended to include medical records, would be contrary to the best interests of the public. Accordingly, we suggest a new provision to be added as 2 MCAR § 1.205 C.1. which would read as follows:

1. A provider may deny parental access to medical data of minors as provided in Minn. Stat. § 144.335.

2. The Responsible Authority may deny parental access to private data when the minor, who is the subject of that data, requests that the Responsible Authority deny such access.

Subsequent paragraphs would then be renumbered accordingly. This, we believe, would remedy the problem described above.

At the hearing, Mr. Gemberling had stated that the Data Privacy Act and the proposed rule were, to the best of his knowledge, harmonious with Minn. Stat. Sec. 144.335 and that there were no conflicts. There is obviously a difference of opinion. Both the Data Privacy Act and Section 144.335 start by defining the "individual" or "patient", in the case of a minor, to include the parent or guardian or person acting in that capacity. The Data Privacy Act, as stated above, includes the exception on release to parents. Such a provision does not appear in 144.335. What does appear is the language previously quoted in Finding No. 19 that the health provider may withhold information from the patient if he reasonably determines that the information would be detrimental to the patient. Given that in the case of a minor patient, the term "patient" means either the minor or his parents or guardian, it is possible to read that provision (as the Minnesota Hospital Association apparently does) to permit the provider to withhold the information from the parent if the provider reasonably determines that the information would be detrimental to the minor. While the Hospital Association has grossly misstated the Department's intent, the proposed rule is not harmonious with Section 144.335. The problem is that the statutes conflict. In resolving this conflict, the Data Privacy Act should be considered the general law, specifying how data on minors will normally be handled. Minn. Stat. Sec. 144.335 is a specific law dealing with the treatment of health records. Therefore, in dealing with health records, 144.335 controls, but the rule does not so provide. The Examiner would recommend that the modification such as that suggested by the Hospital Association should be adopted, but that it should not be limited strictly limited to Minn. Stat. § 144.335, for there may well be other state statutes or federal law dealing with this subject. Such as the following could be added:

1. The responsible authority may deny parental access to private data on a minor pursuant to the provisions of Minn. Stat. § 144.335 or other state statute or federal law that allows or requires the person holding the data to deny parental access if such state statute or federal law provides standards which limit the exercise of the discretion of the person holding the data.

2 MCAR § 1.206 - ACCESS TO CONFIDENTIAL DATA

38. Section 1.206 A. states that access to confidential data is available only to individuals within the entity whose work requires access and to entities and agencies who are authorized by statute or federal law to gain access to that data. /See Finding No. 19 for a suggested modification of this section/. The Department of Commerce, Securities Division, questioned the effect of the rule on investigative data which is, by definition, a type of confidential data. Specifically, they wondered whether information uncovered by the Securities Division during an investigation which indicates illegal activities under the jurisdiction of a different governmental agency could be provided to that agency. Inability to do so would be clearly contrary to public policy. The Securities Division requested that § 1.206 A. be revised to clearly reflect that investigative agencies are authorized to provide evidence of a crime to other appropriate agencies when that evidence is uncovered in an ongoing investigation. (Pub. Ex. 20) The Department should consider the suggestion. The Examiner would hazard a guess that there are state statutes or federal law that require governmental agencies to report discovered evidence of criminal activities to the appropriate authority. If there are not any such laws, then the Examiner would question whether such transfer of information is, indeed, in the public interest, and the legislative intent.

39. Section 1.206 B. requires the responsible authority to establish procedures to assure that access is gained only by appropriate parties and measures by which data subjects shall be informed upon request if they are the subjects of confidential data. The rule goes on to require that the responsible authority take reasonable measures to assure that the person making such an inquiry is actually the data subject. One comment suggested that the clause ". . . or the authorized representative of the data subject," should be added to that provision (Pub. Ex. 5). That appears to be an appropriate modification and should be adopted.

40. At the hearing, counsel for the University of Minnesota noted that the rule did not address a situation addressed in the federal regulations, that is, whether a data subject may be granted access to private data that is contained in an otherwise confidential record. Mr. Gemberling stated that he had not considered such a provision but would think about it.

2 MCAR § 1.207 - ACCESS TO ARREST INFORMATION

41. In the Act, "Arrest information that is reasonably contemporaneous with an arrest or incarceration" is excluded from the definitions of private and confidential data. Therefore, for the duration of time that arrest information is "reasonably contemporaneous", it is, by elimination, public. Section 1.207 A. attempts to make it clear that such data is public for that duration of time by requiring the responsible authority to

"make such information available to anyone who requests it in writing, by personal appearance, by telephone inquiry, or any other means." The Minneapolis City Attorney objected to the telephone inquiry provision:

> This is a bad practice. It not only subjects the person who has been arrested to "crank" calls and announces to the world that he has been taken into custody, but it places a great burden on the police and our office. As to the latter, the bureaucratic difficulties inherent in having someone available who is sufficiently knowledgeable to give arrest information accurately is phenomenal, given that our office handles upwards of 60,000 cases per year. As well, this procedure would, no doubt, affect the police and sheriff's departments in much the same fashion. Finally, the possibilities of miscommunication over the telephone are immense and might well lead to legal action. Perhaps, it would be better to eliminate the telephone inquiry completely. (Pub. Ex. 16)

Being that such arrest information is public, it must be accessible to the public in accordance with the provisions of Minn. Stat. § 15.17, subd. 4. The Department's authority is limited to referring to that statute. See Finding No. 26.

42. Section 1.207 B. defines "duration of time" which, in effect, defines the term "reasonably contemporaneous" found in the Act. This subsection states that the duration of time "commences with the creation or recording of arrest information subsequent to the actual detention or citation of the arrested party" and ends when the arrested person is either released without a criminal complaint being filed or appears before a judicial officer for the offense for which he or she was arrested. The editors of the Minneapolis papers objected strongly, even to the basic approach of this rule.

> We disagree strongly, however, with the interpretation set forth in the Proposed Rules as now written. This is a complex area, and we could get bogged down in detailed discussions of legislative intent and dictionaries and things. But the bottom line is the fact that the Proposed Rules impose a criterion based on the timeliness of a request for arrest data, despite the fact that nothing in the words of the law authorize such a test.
>
> The key phrase in the law is "reasonably contemporaneous." It indisputably modifies the words "arrest information." The plain meaning of the words is that it is the information itself that must be reasonbly contemporaneous with the arrest or incarceration. In other words, the words say that arrest information is the name, age, address, charge, time of arrest, and place of incarceration that are contemporaneous with the arrest. Old aliases, previous addresses, other charges, other jail terms are not covered by this provision.
>
> Given the fact that the words are clear and have a logical meaning that does not contradict other provisions of law, arguments about legislative intent become irrelevant. The Department of Administration is not authorized to rewrite the words of the law to give them a new meaning. That the Proposed Rules are an unreasonable interpretation of the words of the law is attested to by an Attorney General's opinion* that the law does not refer to the timeliness of requests for information, and by the obvious meaning of the words in the law. Of all the provisions of the Proposed Rules, we object most strongly to this misuse of rule-making authority. The rules should be revised to make clear that arrest information about any particular arrest remains public indefinitely, under provisions of this statute.
>
> *Dated Aug. 2, 1976, in response to a question from the Bloomington City Attorney. (Footnote in original) (Pub. Ex. 3)

Despite the editors' and the Attorney General's opinion to the contrary, the interpretation given by the rule of "reasonably contemporaneous" seems more correct. It is difficult to imagine any purpose whatsoever being served by making a legislative distinction between old addresses and new addresses of persons arrested. In fact, under the editors' interpretation, even the old addresses would remain indefinitely public, and the distinction would not exist at all; this interpretation is internally inconsistent. On the other hand, the Department's interpretation that the Act intended to provide an exception so that the Act itself could not be used to foster secret arrests is very reasonable and is effectuated by the definition given in this subsection.

Comments at the hearing and in writing suggested that the beginning of the "duration of time" was not clear. The Minneapolis City Attorney's office listed the following issues.

> Although the information required to be given as "arrest information" is minimal, certain problems do arise in terms of the Rules' definition of "duration of time". Most of these problems will probably arise where people are arrested on several different charges at the same time. It is not unusual for a person to be held on a new offense and have several old warrants outstanding on which he is also in custody. As well, there may be "holds" from several jurisdictions at the time of detention. Given that a person can be held for up to thirty six hours without being charged, several problems could be created. First, the police may not know what the person is "charged" with, since he may not have been charged with anything at that point. Second, the police may not know what information to give out as arrest information if the person is held on both new charges and old warrants. In this regard, the wording of 1.207 B is somewhat suspect, since it states that "duration of time" commences with the "creation or recording" of the information. In this sense, old warrants and new charges might be both created and/or recorded. This could lead to problems of releasing too much information, especially if the warrants are old warrants. Third, the police are the only entity on duty twenty-four hours a day seven days a week. Should an individual be detained on the weekend there would be no interaction with the charging authority who would know what charges are to be filed, if any. Fourth, assuming a person is detained and then released without being charged, it seems to run against that person's right to privacy to release arrest information to all and sundry who desire it. Fifth, to allow arrest information to be released while a person is in custody without having been charged might well lead to a situation where potential witnesses might be harassed, (sic) since the mere arrest of an individual on a given charge might sufficiently alert others involved and prompt them to action. (Pub. Ex. 16)

The Department did not address these concerns specifically at the hearing and may wish to do so. The Examiner would note that if no data is created, the Data Privacy Act does not come into operation. Other laws and rules control the detention of persons without being charged and similar matters.

43. Section 1.207 C. allows the responsible authority to release information other than arrest information in its own discretion and provides some guidelines to be considered by the responsible authorities. The authority for this section is actually based on the discretion granted to responsible authorities in classifying and handling "investigative data". The purpose of the rule is to give some flexibility and provide some guid-

ance to responsible authorities in making public certain data they are not required to make public. Media representatives objected to this provision as giving responsible authorities discretion to decide whether to release data that may, in fact, be public data. As pointed out, the rule, in fact, does just the opposite, and for that reason, is necessary and reasonable. The Department did state in posthearing comments that it would consider modifying or deleting this section entirely.

44. Section 1.207 D. prohibits responsible authorities from making public any data concerning the detention of juveniles except to the juveniles' parents. It was noted at the hearing and by the Ramsey County Commissioners in Public Exhibit 18 that current law allows arresting authorities to release the age and sex of juveniles. This point should be clarified in the rule, especially since the Department has stated that it did not intend to change the discretion afforded to juvenile judges by Minn. Stat. § 260.161 (Dept. Ex. N).

2 MCAR § 1.208 - ACCESS TO INVESTIGATIVE DATA

45. Under Minn. Stat. § 15.162, subd. 2a(b), confidential data on individuals includes data which is:

> Collected by a civil or criminal investigative agency as part of an active investigation undertaken for the purpose of the commencement of a legal action, provided that the burden of proof as to whether such investigation is active or in anticipation of a legal action is upon the agency.

Thus, responsible authorities have some discretion in designating certain data as investigative data. Section 1.208 A. clarifies the statute by stating that investigative data is confidential data and that responsible authorities must comply with section 1.206 concerning access to confidential data.

46. Section 1.208 B. interprets the elements listed by the statute. The Statement of Need and Reasonableness gives the following general introduction to this subsection of the rules.

> To provide guidance to the responsible authority in determining what investigatory data consists of, this section of the rule sets forth three criteria that must be met before any data can be determined to be investigatory data. The confidential classification, as applied to investigatory data, presents a potentially serious problem. As confidential data, investigatory data can be withheld from both data subjects and the general public. This condition prevents the operation of checks on agency abuse represented by either the subject's demand for correction or the possibility of public exposure through public access. Therefore, it is necessary that this exercise in discretion operate within the tightest possible guidelines. The rule presents those guidelines as criteria that must be met before any data can be designated as investigatory data. The criteria are drawn from the implied definition of investigative data found in 15.162, Subdivision 2a.
>
> The three criteria that must be met are referred to in the rule as: 1) the collecting agency criteria; 2) the purpose of collection criteria; and 3) the active data criteria. Requiring the responsible authority to determine that the data in question can meet all of the criteria is the method adopted by the rule to assure that this exercise in administrative discretion operates within the requirements of the Act, and with the minimum possible abuse of discretion.

47. Section 1.2 B.1. deals with the "collecti agency" criteria. One of the types of agencies specifically listed by the rule is "any agency given statutory authority to revoke or suspend licensure." Several state agencies who make investigations and take actions different from license discipline suggested that this item should be broadened or another item added to cover their particular situations. There are, for example, other forms of authority granted by state agencies in addition to licensure. These include granting of charters, certificates of authority, permits and registration. Several agencies also have authority to prohibit certain activites by individuals and entities who have not been granted the proper authority through the issuance of cease and desist or similar orders. Other agencies have the authority to assess fines for inappropriate activities. All these actions are invariably the result of some form of investigation by the agency which may, or may not, be required to be conducted with some degree of secrecy in order to be effective. This section of the rule should be clarified to include all agencies who may take any of these similar actions.

48. Section 1.208 B.2. clarifies the meaning of "legal action" by listing several examples. The editors of the Minneapolis papers objected strenuously to broadening the definition of "legal action" beyond the standard definition of "any proceeding in any court of this state," found in Minn. Stat. § 645.45 (Pub. Ex. 23). The Examiner agrees with the Department and with the Department's counsel (Dept. ex. M) that the context in which the word is used indicates that a broader definition was intended and that the proposed rule is necessary and reasonable to clarify that intent.

Again several agencies requested further clarification as to the application of this subsection to certain types of investigations, including presentence investigations and diversion programs, cease and desist orders, fines and discipline against charters, certificates of authority, and registration. The Examiner would again recommend that these matters be more clearly included in the rule.

49. Section 1.208 B.3. deals with the "active data" criteria. This particular rule is one of the best examples of the reasonable results obtained by the Department in attempting to balance extremely divergent views of the statute. The editors of the Minneapolis papers point out that some government officials have attempted to try to apply the words of the statute to any fact-gathering process that might sometimes lead to an investigation. They cite the example of police departments keeping records of complaints telephoned in by the public and attempting to classify such records as investigative under the Act. They call this an abuse (Pub. Ex. 23). Another view of that type of data was expressed by Paul J. Tschida, Superintendent of the Bureau of Criminal Apprehension:

> The appropriate investigative agency has the responsibility to accept information regarding possible criminal activity and to resolve such allegations as time and resources allow. Such information clearly should not be made public until an arrest is made and the relevant information is revealed as part of a court process.

> "If a case goes to trial, the prosecutor, and ultimately the court, make determinations as to relevancy and whether the individual's right to privacy must succumb to the state's and the defendant's interests in resolution of the criminal charge. If the matter is otherwise resolved, I can see no overriding public interest in surfacing information which is so often damaging to character and reputation. (Pub. Ex. 10)

The Minneapolis City Attorney suggests that criminal actions may remain active after all perpetrators have been apprehended, the statute of limitations, and all rights of appeal have been exhausted. The City Attorney then suggests that the rule should allow more discretion to the agency to determine on a case-by-case basis whether or not the invesigation is in "active" status or not.

The Examiner finds that the criteria given in the rule are not unreasonable for the reasons given in the Statement of Need and Reasonableness.

50. The Hennepin County Attorney's office pointed out a typographical error in section 1.208 B.1.a.; the reference in that section should be to 2 MCAR § 1.202 B.1.

2 MCAR § 1.209 - ACCESS TO SUMMARY DATA

51. Section 1.209 D.1. requires the responsible authority to respond to a written request for preparation of summary data within ten days of such request by either (a) providing the summary data requested, (b) providing a statement to the requestor describing a time schedule for preparing the requested summary data, or (c) providing access to the requestor to the private or confidential data for the purpose of the requestor's preparation of the summary data. The third option raised the most concerns in this particular rule. The Hennepin County Attorney's office suggested that it should be made absolutely clear that the choice of the three options was up to the responsible authority. The Ramsey County Commissioners, the Ramsey County Welfare Department, and the Minnesota Association of Community Mental Health Programs, Inc., were all concerned that the protections provided by the rule were inadequate to prevent access to private and confidential data by inappropriate persons (Pub. Exs. 18, 25 and 39). This same concern was raised at the hearing.

This rule is an attempt to implement the provisions of Minn. Stat. § 15.1641(d) which provides in part:

> The responsible authority may delegate the power to prepare summary data to the administrative officer responsible for any central respository of summary data, or to a person outside of its agency if the person agrees in writing not to disclose private or confidential data on individuals.

Mr. Gemberling stated at the hearing that the statute is permissive, that is, it states that the responsible authority may delegate the power to prepare summary data to a person outside of the agency and that the purpose of the provision is to prevent the Data Privacy Act from thwarting the efforts of researchers into government processes. It was requested at the hearing that the rule be clarified to indicate that the responsible authority may restrict outside persons to qualified researchers or a similar person for "research type" purposes. The Examiner would recommend that language similar to that suggested be added to the rule so that responsible

authorities are absolutely clear that they may reject the request of any person for access to confidential or private data for the supposed purpose of preparation of summary data. It is possible under the present language for a person interested in confidential data on a particular individual to gain access to that data by requesting preparation of summary data; there should be some attempt by responsible authorities to assure that the outside person is really only seeking summary data. A non-disclosure agreement is little security.

52. Section 1.209 B.5. describes various methods of preparing summary data. Included within the rule under § 1.209 B.5.c.(3) is removing all unique personal identifiers by "programming computers in such a way that printed or terminal output does not contain personal identifiers." The manager of the Information Service Division of the Department of Administration points out that there are several forms of output media from computers not embraced by the underlined term. He suggests, and the Examiner agrees, that the term should be broadened. Perhaps the underlined term could be changed to "output in any form".

2 MCAR § 1.210 - CLASSIFICATION OF DATA

53. This proposed rule states that in order to comply with the Act, responsible authorities must classify the data in their control and gives four steps for doing so: (a) review all types of data maintained, active and inactive; (b) determine the private, confidential or public classification of each type of data; (c) identify a state statute or federal law supporting the determination of private of confidential; and (d) administer the data in accordance with the determinations made. The Dakota County Attorney offered the following comment:

> It is our contention that this rule both exceeds statutory authority and is unnecessary. While Minn. Stat. § 15.163 speaks of preparing a public document describing each category of record, file, or process, a close reading of the statute shows that such a requirement exists only for private and confidential data and not for public data, as would be required under § 1.210. We are well aware of the fact that Minn. Stat. § 15.1641(e) requires the Responsible Authority to establish procedures and safeguards to ensure that all public, private or confidential data on individuals is accurate, complete and current. However, we do not believe the mandate of this statute gives the Department of Administration the rule making authority to establish such procedures and safeguards for the Responsible Authority, as 2 MCAR § 1.210 attempts to do. Minn. Stat. § 15.1641(e) specifically places this burden upon the Responsible Authority and not upon the Department of Administration. It should be noted that Minn. Stat. § 15.1671 which gives the Commissioner of Administration the power to implement the enforcement and administration of the Data Privacy Act, does not give the Commissioner authority to supersede any provision of such Act. We believe 2 MCAR § 1.210 is an attempt to supersede the discretion granted in the statute to the Responsible Authority. Additionally, the implementation of the provisions of Minn. Stat. § 15.163 is satisfactorily taken care of in 2 MCAR § 1.214. Hence, we see no need whatsoever for 2 MCAR § 1.210 and respectfully request you to delete this section in its entirety in your report. Deleting this section would eliminate a great deal of the implementation cost of complying with these rules in addition to making these rules consistent with the Data Privacy Act. (Pub. Ex. 31)

The Department has the authority to adopt this rule, for it is a method of implementation of the Data Privacy Act. The Statement of Need and Reasonableness offered the following justification for this rule:

> Sections A through D of this rule set forth the reasonable steps that should be taken to comply with the classification requirement. The steps to be taken are a logical progression beginning with identification of all the data being maintained by the agency. If these steps are not followed, the appropriate actions taken by the responsible authority, it will be impossible for the agency to comply with the detailed requirements of the Act.

This rule amounts to the Department's suggestion as to the best way for responsible authorities to comply with the requirements of the Act. Normally, such suggestions should not be elevated to rule status - they become too inflexible. However, given the many requests for guidance made by responsible authorities, even on the smallest details, this rule is necessary and reasonable.

54. Several persons at the hearing and in written comments objected to the requirements to review inactive data and to determine "public" classifications as being unnecessary and very expensive (Pub. Exs. 12, 18 and 28). It was suggested that there would be little objection if the rule merely required reviewing active data and determining classifications for only private or confidential data.

The Ramsey County Commissioners had the following comment in regard to inactive data:

> This provision is extremely expensive in terms of staff hours. The provisions in 1.210 A requiring a review of active and inactive data puts upon local governmental units and departments the apparent duty of going into archives closed record systems, and any record storage area to classify whatever information is there. This is a near impossible task and we recommend that the words "and inactive" be deleted from 1.210 A. We base this opinion on the fact that on the rare occasions when access is needed, data specifically requested could be reviewed and classified according to the "active" file procedures outlined by this law. To do otherwise might well require thousands of staff-hours to review literally hundreds of thousands of documents which are almost never asked for. Such a requirement is incredibly wasteful in terms of staff time and effort. It's cost is outrageous, whether it be born (sic) by local or state taxpayers. Again we note this burden is placed upon local governmental units with no state provision for reimbursement. (Pub. Ex. 18)

The task is not really so burdensome because the entities only have to look at record "types", and there is some time limit on what records could be expected to contain unique identifiers of living persons. Whether all inactive data must be reviewed depends upon whether such data must be listed on the § 15.163, subd. 1, list (See Finding 57). Since that statute requires a list of all private and confidential data maintained by the entities, the entire problem hinges on whether inactive data is being "maintained". The Department's apparent position that even inactive data is being "maintained" and must therefore be reviewed and listed is a reasonable reading of the statute. Any change here should be requested from the Legislature.

As the Dakota County Attorney pointed out above, the real need is to identify private and confidential data in order to comply with the reporting and handling requirements of the Data Privacy Act. It was, however,

classifying data as "public" that seemed to cause the most problems for the political subdivisions. This again stemmed from the so-called "gap theory" which makes responsible authorities unsure of whether something is really public or not. If the so-called gap is deleted as suggested in Finding No. 18, then this objection to this rule would also be eliminated. However, it may still be reasonable to simply delete the requirement here to classify anything other than private and confidential data, and the Examiner would so recommend.

55. Counsel for the League of Minnesota Cities pointed out at the hearing that municipalities had not budgeted for the expenses of complying with these rules during the current year, and so requested that a 12 to 18-month delay be built into all the requirements these rules will be imposing upon responsible authorities. The Department indicated at the hearing that it would consider putting a delay on this particular rule.

2 MCAR §§ 1.211, 1.212 and 1.213 - AUTHORITY, APPOINTMENT AND APPOINTMENT POWER OF THE RESPONSIBLE AUTHORITY.

56. There were few comments on these sections. Counsel for the League of Minnesota Cities called all three good and necessary clarifications of the duties of responsible authorities. These three sections are reasonable and necessary for the reasons given in the Statement of Need and Reasonableness.

2 MCAR § 1.214 - DUTIES OF THE RESPONSIBLE AUTHORITY RELATING TO PUBLIC ACCOUNTABILITY

57. Minn. Stat. § 15.163, subd. 1, states:

> On or before August 1, 1976, the responsible authority shall prepare a public document containing his name, title and address, and a description of each category of record, file, or process relating to the private or confidential data on individuals maintained by his state agency, statewide system, or political subdivision. 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 keep it accurate.

The proposed rule implements that section of the statute by first requiring that until the list required by the statute has been prepared or updated, the responsible authority must post a notice identifying himself or his designees as the persons responsible for answering inquiries concerning provisions of the Act, and secondly, by describing what the list required by the Act must contain.

In describing the contents of the list, the Department departed from the statutory language, ". . . a description of each category of record, file or process", and provided the following in § 1.214 B.:

> In the public document to be prepared or updated by August 1 of each year as required by section 15.163 of the Act, the Responsible Authority shall identify and describe all records, files, or processes maintained by his entity, which contain private or confidential data.

The Department stated at the hearing that it did not use the word "category" because it did not find it particularly helpful in describing what had to be listed. However, as pointed out at the hearing, and in several

comments (Pub. Exs. 12, 18, 25 and 33), the language of the proposed rule can be read to require that the responsible authority review and identify on the list every individual file or record which he maintains. The example given at the hearing was that the responsible authority would not merely have to identify personnel records as containing private data, but would have to identify each and every employee's personnel record on the list. Mr. Gemberling stated that that was not his intent and pointed to the sample form printed at 3 State Register 365 to show that the rule actually intended to address types or categories, as the word is used in the statute, of files and records rather than each individual entry within that file or record. Being that the rule is possibly confusing to a number of persons, it should be clarified by some means to indicate that not every individual data entry has to be identified and listed. In § 1.215 C.1., the language used is, ". . . for each type of record, file or process. . .". That would also be appropriate here. Or perhaps the Act's use of the word "category" is the best that can be hoped for.

58. Several persons thought this rule would be a high expense item for the political subdivisions. However, those comments seemed to be based primarily on the confusion just discussed and the expense that would be encountered if every individual data entry had to be reviewed and listed. Properly interpreted and having the rule clarified will eliminate most of the anticipated cost of this particular rule. It should further be noted that the rule does not add anything to the requirements that already exist in the statutes except for the minimal requirements of requiring citation of authority to withhold data and identification of designees of the responsible authority.

2 MCAR § 1.215 - DUTIES OF THE RESPONSIBLE AUTHORITY RELATING TO THE ADMINISTRATION OF PRIVATE AND CONFIDENTIAL DATA

59. Minn. Stat., § 15.1641(c) states:

> Private or cofidential data on individuals shall not be used, collected, stored or disseminated for any purposes other than those stated to an individual at the time of collection in accordance with section 15.165 or, in the case of data collected prior to August 1, 1975, for any purpose other than those originally authorized by law, unless (1) the responsible authority files a statement with the commissioner describing the purpose and necessity of the purpose with regard to the health, safety or welfare of the public and the purpose is approved by the commissioner, or (2) the purpose is subsequently authorized by the state or federal legislature, or (3) the purpose is one to which the individual subject or subjects of the data have given their informed consent.

This section of the rules defines and clarifies the procedures responsible authorities must follow in order to comply with the statute and also with the duties imposed upon responsible authorities by Minn. Stat. §§ 15.1641(b) and 15.165. The logical first step in this process is for each responsible authority to determine the purposes for the collection of private or confidential data and the legitimate uses of such data. However, as can be seen from the statute, that may depend upon whether the data was collected prior to or after August 1, 1975. Therefore, the first requirement of § I.215 is:

> In order to administer the requirements of § 15.1641(c) of the Act, the Responsible Authority shall determine for each record, file, or process identified in 2 MCAR § 1.214 whether the data contained therein was collected prior to or subsequent to August 1, 1975.

It first should be noted that the items identified under § 1.214 are types or categories of records, files and processes, and so the language here should be changed to state, ". . . for each type of record, file, or process identified. . . " It might further be noted that technically, the rule never tells what happens to data collected on August 1, 1975. References to data collected "subsequent to August 1, 1975," should state, "on or subsequent to August 1, 1975."

60. Section 1.215 A. relates to records, files and processes containing data collected prior to August 1, 1975 and requires the responsible authority to review the legal authorities which required that private or confidential data to be collected, determine the lawful purposes for collection of the data at the time it was collected, and direct the staff of the entity that such data may be used or or disseminated only for those lawful purposes. Similarly, for data collected since August 1, 1975, § 1.215 B. requires the responsible authority to review the legal authority which requires the collection of the data and identify the purposes for the collection of and the intended uses of such data that have been or should have been communicated to the data subjects when the data was collected.

Several agencies objected to the expense that the requirement for reviewing pre-1975 data would generate (Pub. Exs. 12, 26, 28 and 33). They all recommend that such data could be reviewed for legal authority purpose and intended use whenever it was requested or needed to be used. The basic reason is that many agencies have many, many files and records which are stored away in some basement and never used.

It is difficult for the Examiner to understand how the duties imposed regarding pre-1975 data could add much cost for the political subdivisions. There may be some confusion as to whether the rule requires review of each individual piece of data, but the rule only requires a review for each type of record, file or process identified in 2 MCAR § 1.214. If those items have already been identified for § 1.214, then the responsible authority already knows what each of those items is and the legal authority for its classification as private or confidential.

The Minnesota School Boards Association pointed out (Pub. Ex. 14), there may be some types of records that contain data collected both prior to and subsequent to 1975. No particular burden is created there because it would generally be the same legal authority that stated the purpose for collection and legal uses of that data, regardless of when it was collected.

61. Section 1.215 C. requires the responsible authority to use the purposes and uses identified in either of the two prior subsections to (1) prepare lists which identify the uses and purposes for each type of record, file or process identified under § 1.214, and (2) to make the purposes and uses known by any of a number of methods to persons from whom data, private or confidential, is collected. The Minnesota School Boards Association questioned whether the responsible authority becomes civilly liable if, for

instance, a person or entity authorized by federal law to receive any data disseminated from the record is not listed (Pub. Ex. 14). The Department replied that the liability may very well be present but would arise from the entity's violation of Minn. Stat. §§ 15.165, subd. 2, or 15.1641(b) and (c) (Dept. Ex. O). This rule provides a method by which responsible authorities can be more certain of complying with the requirements of the Act and is reasonable as proposed.

2 MCAR s 1.216 - DUTIES OF THE RESPONSIBLE AUTHORITY AS THEY RELATE TO THE ADMINISTRATION OF ALL ENTITY DATA.

62. Most of this section of the rules deals with the steps responsible authorities must take in order to be able to comply with Minn. Stat. s 15.164 (b) which limits collection and storage of all types of data on individuals and use and dissemination of private and confidential data on individuals to that "necessary for the administration and management of programs specifically authorized by the Legislature, local governing body or mandated by the federal government." The method adopted by the rules is to require responsible authorities to formulate a plan for review and analysis of their data administration practices within 18 months of the effective date of these rules.

63. Section 1.216 A. requires that the plan at least provide for the preparation of a list of, or index to, all data or types of data currently collected, stored, used or disseminated by the entity. The list or index must include identification of the laws that authorize the programs or functions for which the data is collected or which authorize the actual data collection, storage, use or dissemination; must be updated when new or different collection, storage, use or dissemination is authorized; and must be available to members of the general public upon request.

Mr. Gemberling stated at the hearing that this section could well be the most expensive to political subdivisions of any of the requirements of the proposed rules, and that concern was expressed by a number of persons (Pub. Exs. 18, 27 and 33). Counsel for the League of Minnesota Cities again requested that this rule be made clear to the effect that the list or index was not to all data elements but to the categories or types of data maintained by the agency. This should be clarified.

64. At the hearing, counsel for the League of Minnesota Cities opposed requiring "stored" data to be indexed because it would be a very expensive and difficult task. As Mr. Gemberling pointed out at the hearing however, the statute refers to the storage of data, and so such data must be reviewed in order to comply with the requirements of Minn. Stat. § 15.1641(b). (See Finding No. 54)

65. Section 1.216 D. implements the requirements of Minn. Stat. § 15.1641(e) that requires responsible authorities to establish procedures and safeguards to ensure that all public, private or confidential data on individuals is accurate, complete and current. It does so by defining the terms "accurate", "complete" and "current". The Department of Economic Security suggested that more clarification was needed as to the administrative process that is necessary to review and correct inaccurate or in-

complete records. It was pointed out in the Statement of Need and Reasonableness that the previous versions of this rule, though perhaps not this particular section, were much more detailed in the specific steps required to be in the responsible authorities' plan. That specificity was criticized because it could be enormously expensive for some particular responsible authorities and because it was not flexible enough for all the various types of governmental entities who may be responsible authorities. In a similar vein, it is not unreasonable for the Department not to specify every specific step for this particular section of the plan.

2 MCAR § 1.217 - DUTIES OF THE RESPONSIBLE AUTHORITY AS THEY RELATE TO COMPUTERIZED DATA

66. Minn. Stat. § 15.1641(e) states in part:

> Emphasis shall be placed on the data security requirements of computerized files containing private or confidential data on individuals which are accessible directly via telecommunications technology, including security during transmission.

This section of the rules implements that statute by requiring an audit of the security measures within 180 days of the effective date of these rules and on an annual basis and then provides some examples of appropriate security measures. Again, some concern was expressed as to the cost of implementing this rule. In particular, the Department of Economic Security stated that the requirement for an audit within 180 days may cause extra expense where there has been an audit within the last year (Pub. Ex. 17). It would seem reasonable that if an audit within the previous year adequately assessed the concerns expressed in the rule, it should not have to be performed again, except on the annual basis. The Examiner would recommend that language to that effect be added to the rule.

67. The manager of the Information Systems Division of the Department of Administration pointed out that the rule refers to the integrity of "directly accessible files". He stated:

> I feel this term may communicate that not all of the data stored in ISD, or in any of the other data processing centers serving state agencies, is at risk. This is not so. Advances in data processing technology have put capabilities in the hands of people outside of data processing centers that allow access to all of the data maintained at the center.

The statute says that emphasis should be placed on files that are accessible directly, but it does not state that files otherwise accessible should be ignored . However, the definition of "directly accessible files" in § 1.217 A. means all files to which access can be made or updating performed through use of any type of communications terminal. That again may be too narrow as access may be achieved through other than communications terminal, such as simply by walking into the data center and picking up a magnetic tape and leaving. The Examiner would recommend that § 1.217 A., the definition of "directly accessible files" be deleted and that § 1.217 B. be modified to read:

> Within 180 days of the effective date of these rules, the Responsible Authority shall perform an audit of the physical and softwear security measures that the entity has installed to protect the integrity of computerized files containing private or confidential data on individuals.

2 MCAR § 1.218 - ADMINISTRATIVE APPEAL

68. This rule clarifies the provisions of Minn. Stat. § 15.165, subd. 4, by stating that the administrative appeal provided for by the Act shall be to the Commissioner of Administration. Section 1.218 C. provides:

> The Department of Administration shall be reimbursed for all costs associated with Contested Case Proceedings by the entity whose Responsible Authority has been the impetus for the individual's appeal to the Commissioner of Administration.

Almost all the political subdivisions thought this was unfair and unreasonable (Pub. Exs. 14, 16, 18, 26, 29, 30 and 32). The Department's reason for this procedure is that it does not have the funds to pay the cost of contested case proceedings, itself. Unless the costs are billed to the agencies, the appeal mandated by the statute cannot be provided. The main objection to this provision is that the political subdivisions would have to bear the costs of frivolous and unwarranted appeals. In response to that, the Department pointed out that it believed that the Commissioner must make a determination as to whether it was appropriate to convene a contested case proceeding and that they seriously doubted that he would do so in the instance of a frivolous or unwarranted appeal. The Department suggested that it was open to the possibility of adding words to that effect in the proposed rule (Dept. Ex. O). It is not absolutely necessary to so provide in this rule because the rules of the Office of Hearing Examiners in 9 MCAR § 2.203 C.4. grant hearing examiners the authority to hear and rule on motions. Such motions have often included motions to dismiss a contested case for any number of reasons. If the Department does desire to include such a provision within the rule, the Examiner would suggest the following language which was adapted from the procedural rules of the Department of Human Rights:

> The Examiner, at any stage of the proceedings, after all parties have had an opportunity to present their views, may recommend dismissal of any sham, capricious, or frivolous case, or any case not within the jurisdiction of the Department.

Such a provision would not eliminate all hearing costs, but it would provide a method to avoid unnecessary costs.

2 MCAR §§ 1.219 - GENERAL POWERS OF THE COMMISSIONER OF ADMINISTRATION; 1.220 - DUTIES OF THE COMMISSIONER OF ADMINISTRATION RELATING TO EMERGENCY CLASSIFICATION OF DATA; and 1.221 - SEVERABLE PROVISIONS

69. These sections are necessary and reasonable for the reasons given in the Statement of Need and Reasonableness.

COSTS OF IMPLEMENTATION

70. Many comments were made concerning the cost to implement the proposed rules (Pub. Exs. 9, 12, 14, 15, 16, 18, 19, 27, 31, 32, 36 and 37). As has been noted in the previous findings, many of the costs estimates were based upon misinterpretations of the rules or can be resolved by the clarifications and modifications to the rules suggested in the previous Findings. Even if the Department adopts all the recommendations made by the Examiner, or makes other cost-savings changes of its own, the costs of implementing the Data Privacy Act will still be significant. As pointed

out by counsel for the League of Minnesota Cities at the hearing, these rules will help focus and better define what the costs will actually be and should aid those responsible for public funding to make the appropriate decisions.

CONCLUSIONS

1. Due, timely and adequate legal notice of the hearing was properly served and published by the Department. All other procedural requirements of statute and rule have been fulfilled.

2. Except as noted in the Findings, the Department has demonstrated its statutory authority to adopt the proposed rules.

3. Except as noted in the Findings, the proposed rules fulfill substantive requirements of statute and rule.

4. Except as noted in the Findings, the Department has demonstrated that the proposed rules are necessary and reasonable.

5. The recommendations made by the Examiner in the Findings are not intended to in any way preclude the Department from making its own non-substantial changes or improvements to the rules.

RECOMMENDATION

The Hearing Examiner recommends that the proposed rules be modified as suggested in the Findings, and that so modified, they be adopted.

Dated this 5th day of February, 1979.

STEVE M. MIHALCHICK
Hearing Examiner

Testimony of Ramsey Action Programs, Inc., Regarding Proposed Rules Governing the Enforcement and Administration of the "Minnesota Data Privacy Act"

October 31, 1978

My name is Dr. Charles Schaffer, and I am the Director of Resource Development for Ramsey Action Programs, Inc., of Saint Paul -- a private, non-profit community action agency operating in the County of Ramsey. My comments today are on behalf of Ramsey Action Programs and the Minnesota Community Action Agency Executive Directors' Association. Both organizations wish to express their concern with certain portions of the proposed text of 2MCAR 1.201-1.220 as published in the State Register of Monday, September 4, 1978.

Although most community action agencies operating in the state of Minnesota are private, non-profit corporations, they are very much affected by these proposed rules. Minnesota Statutes 15.162 subd.5 specifically extends coverage of that act (the Minnesota Data Privacy Act) to non-profit community action agencies, defining them as political subdivisions for the purposes of the act.

Our major concern is with the nature of the definitions of "private data" and "confidential data" in the proposed rules. Specifically,

the proppsed rules are silent themselves with regard to definitions and standards for classifying data and instead rely on federal or state statutes to provide definition. Thus 2MCAR 1.202D states that "Confidential Data as defined in §§ 15.162 subd. 2a of the Act shall only include data which is expressly classified by either a state statute, including the provisions of §§ 15.1642 of the Act, or federal law." Likewise, 2MCAR 1.202E states that "Private Data, as defined in §§ 15.162, subd. 5a of the Act, shall only include data which is expressly classified by either a state statute, including the provisions of §§ 15.1642 of the Act, or federal law."

Furthermore, the text of 2MCAR 1.202D(3) and 2MCAR 1.202E(2)(b) would indicate that only a statutory basis can cause data to be classified as "confidential" or "private;" that an administrative rule, regulation or decision is not sufficient.

These proppsed regulations pose serious difficulties for community action agencies which, in the course of their day-to-day administration of federally sponsored anti-poverty activities, collect a considerable amount of data on program participants: data which deals with the economic, social and personal circumstances of participants and their families. Community action agencies have

always treated this kind of information as private even though there is most often not a statutory basis, or an administrative rule basis, for that classification. The present proposed rules would, in the absence of state or federal statutory authority, prohibit that kind of information from being classified as private.

When the proposed rules first appeared, Ramsey Action Programs sought the opinion of the Office of the General Counsel of the Community Services Administration -- the federal agency which provides most funding and program direction to community action agencies. Our inquiry was whether the provisions of the Code of Federal Regulations or the Federal Data Privacy Protection Act extended adequate protection to data collected by community action agencies. In the opinion of the CSA General Counsel's Office those provisions did not offer adequate safeguards. I would like here to read into the record the text of that opinion.

Based on these findings and opinions we would ask that the proposed text of 2MCAR 1.202A-1.202E not be adopted and that the Commissioner of Administration develop new sections providing for clear standards of classification of data and allowing for state or federal administrative rules to be used as a basis for classification of data.

Community Services Administration
WASHINGTON, D.C. 20506

18 OCT 1978

Dr. Charles A. Schaffer
Director of Resource Development
Ramsey Action Programs, Inc.
509 Sibley Street
St. Paul, Minnesota 55101

Dear Dr. Schaffer:

This is in response to your letter of October 12 asking the opinion of this office as to whether the general provisions of OEO/CSA Instruction 7041-1 (45 CFR 1070.1) provide adequate protection for private data collected on individuals by CAA's under the provisions of Minnesota Statutes 15.162 - 15.174 and proposed rules 2 MCAR 1.201 - 1.221.

As we discussed in our conversation of October 16, Minnesota Statute 15.162, subd. 5 defines CAA's as "political subdivisions" for the purpose of this legislation. Consequently they are governed by the provisions of the proposed rules classifying data as public, private, or confidential. We find these rules confusing, but our review of the rules and the underlying statute indicates that they do not sufficiently protect the personal privacy of individuals, especially program recipients. The only clear protection is that for data which is private or confidential under Federal statute; however, the Privacy Act (5 U.S.C. 552a) does not extend to grantees.

Under proposed 2 MCAR 1202 E (2)(b), a CSA regulation would appear not to provide protection. Furthermore, 45 CFR 1070.1-5 only protects privacy by implication, stating: "Except in cases where disclosure of documents would involve an invasion of privacy...the agency should permit examination and inspection of all such documents." Nevertheless, CSA policy is firmly in support of the fullest possible protection of personal privacy. We are considering the addition of a new subsection to 45 CFR 1070.1 to implement this CSA policy more effectively.

Sincerely,

John C. Meyer

John C. Meyer
Assistant General Counsel

STATEMENT BY RALPH J. MARLATT
PRESIDENT
OF THE
INSURANCE FEDERATION OF MINNESOTA

BEFORE THE

DEPARTMENT OF ADMINISTRATION
DATA PRIVACY UNIT

CONCERNING

PROPOSED RULES GOVERNING THE
ENFORCEMENT AND ADMINISTRATION
OF THE
"MINNESOTA DATA PRIVACY ACT"

ST. PAUL, MINNESOTA
OCTOBER 31, 1978

MR. COMMISSIONER, MY NAME IS RALPH J. MARLATT AND I AM PRESIDENT OF THE INSURANCE FEDERATION OF MINNESOTA. THE FEDERATION IS A TRADE ASSOCIATION REPRESENTING 43 LIFE, HEALTH, PROPERTY AND CASUALTY INSURANCE COMPANIES. 29 OF THESE COMPANIES ARE DOMICILED IN THE STATE OF MINNESOTA. WITH ME TODAY IS DR. WARREN KLEINSASSER, SECOND VICE PRESIDENT & CHIEF MEDICAL DIRECTOR, MINNESOTA MUTUAL LIFE INSURANCE COMPANY.

THE INSURANCE FEDERATION IS CONCERNED THAT THE PROPOSED RULES GOVERNING THE ENFORCEMENT AND ADMINISTRATION OF THE "MINNESOTA DATA PRIVACY ACT" GOES WELL BEYOND WHAT IS REQUIRED BY CURRENT LAW.

THE PROBLEM IS THAT THE PROPOSED RULES APPEAR TO COVER GOVERNMENTAL ENTITIES DEFINED BY MINNESOTA STATUTES SEC. 15.1671, SUBD. 5, 7 and 8 (SEE 2 MCAR SEC. 1.201), WHICH INCLUDES STATE HOSPITALS AND THE UNIVERSITY HOSPITAL. THUS, THE RULE SEEMS TO REQUIRE THAT WE HAVE A NOTARIZED AUTHORIZATION IN ORDER TO OBTAIN RECORDS FROM THESE HOSPITALS. IT SEEMS TO ME THE NOTARIZATION PROVIDES LITTLE PROTECTION FROM FRAUDULENT ACCESS AND UNDULY INCREASES THE EXPENSE FOR CLAIMANTS AND APPLICANTS FOR INSURANCE.

THERE ARE, OF COURSE, DRAMATIC EXAMPLES THAT HAVE BEEN DISCLOSED IN THE MEDIA OF IMPROPER ACCESS BEING GRANTED. THESE, I BELIEVE, ARE VERY FEW IN NUMBER, THOUGH OBVIOUSLY UNFORTUNATE WHEN THEY OCCUR. ONE HAVING AN INTENT TO GAIN SUCH ACCESS WOULD HAVE LITTLE TROUBLE OBTAINING OR FEIGNING A NOTARY'S SEAL, AND THE PENALTIES FOR THE ACT WOULD BE NO MORE STRINGENT IF THE IMPROPER NOTARIZATIONS WERE DISCOVERED. MEANWHILE, HUNDREDS OF NOTARIZATIONS WOULD HAVE TO BE OBTAINED CAUSING UNDUE EXPENDITURE OF MONEY AND TIME, AS WELL AS DELAYING THE PAYMENT OF CLAIMS AND THE UNDERWRITING OF INSURANCE POLICIES DESIRED BY APPLICANTS.

SUBSTITUTE LANGUAGE MIGHT BE CONSIDERED WHICH WOULD REQUIRE THAT REASONABLE EFFORTS BE MADE TO DETERMINE THAT ONLY VALID SIGNATURES ARE RECOGNIZED, OR AN EXCEPTION FROM THE RULE SHOULD BE GRANTED FOR HOSPITAL RECORDS WHICH ARE SO OFTEN USED IN ORDER TO PAY CLAIMS AND UNDERWRITE POLICIES IN THE INTEREST OF THE SUBJECT OF THE DATA.

ON THE PROPERTY AND CASUALTY SIDE, ARSON SEEMS TO BE THE ONLY PROBLEM AREA. INSURANCE COMPANIES MAKE NUMEROUS CONTACTS EACH YEAR WITH FIRE MARSHALS IN THE COURSE OF AN ARSON INVESTIGATION. BECAUSE OF THE PRIVACY LEGISLATION, SOME MARSHALS HAVE BEEN RELUCTANT TO PROVIDE NEEDED INFORMATION. THE MINNESOTA INSURANCE COMPANIES MUST HAVE ACCESS TO THIS INFORMATION IF ARSONISTS ARE TO BE APPREHENDED AND PROSECUTED. NEW LANGUAGE SHOULD BE ADDED TO THE PROPOSED RULES TO MAKE IT CLEAR THAT FIRE MARSHALS ARE EXEMPT OR WILL RECEIVE IMMUNITY WHEN GIVING OUT THIS TYPE OF INFORMATION.

THE INSURANCE FEDERATION OF MINNESOTA WOULD APPRECIATE YOUR FAVORABLE CONSIDERATION OF ITS CONCERNS.

ERRATA

to the proposed adoption of permanent rules governing the enforcement and administration of the "Minnesota Data Privacy Act", as published in the State Register, September 4, 1978

Page 347:

Rule 2 MCAR § 1.201, Subsection A, should read: "A. These rules shall apply to those governmental entities as defined by Minn. Stat. § 15.162, ..."

Pages 348-349:

Rule 2 MCAR § 1.202, Subsection E. following l.c., the Rule should read:

2. Data is not private if:

    a. A federal agency rule provides substantially that as a part of its plan for implementation of a certain federal program, a state agency, statewide system, or a political subdivision must provide for the confidentiality of data obtained from program subjects.

3. A state agency rule, an executive order, an administrative decision, or a local ordinance shall not classify data as "private", or use wording to make data inaccessible to the public unless there is a state statute or federal law as the basis for the classification.

Page 350:

In Rule 2 MCAR § 1.202, Section L. 3., paragraph a. should read:

    a. The commissioner of any state department or any executive officer designated by statute or executive order as responsible for such a system; or

Page 353:

In the introductory paragraph of 2 MCAR § 1.208, change the second to the last word in that paragraph from investigatory to investigative.

In 2 MCAR § 1.208, Section A. change the first word of that paragraph from Investigatory to Investigative.

Page 345:

Rule 2 MCAR § 1.209. The first sentence in the introductory paragraph should read: "Pursuant to Minn. Stat. § 15.1641 (d), ..."

Page 355:

Rule 2 MCAR § 1.210, the fourth paragraph should be denominated as D. instead of B.

ADMIN 1000

STATE O NNESOTA

DEPARTMENT OF ADMINISTRATION

Office Memorandum

TO : Steve Mihalchick
Hearing Examiner's Office

DATE: November 20, 1978

FROM : Don Gemberling
Data Privacy Unit

PHONE: 296-6733

SUBJECT: Response to Minnesota School Board's Association Comments on the Proposed Rules

Introduction:

Although some of the comments made by the Minnesota School Boards Association (MSBA) may be helpful to us in our final review of the rules, generally we find the comments to be argumentative, highly general in nature, lacking in specifics to support general conclusions, and more critical of the underlying legislation than of the proposed rules themselves. Clearly, if MSBA can point out to you that there are rules that have exceeded the command of the statute then you should so inform us in your final report. As we said at the Public Hearing, we have taken care to write these rules as closely as possible to the requirements of the Statute. I have numbered and lettered my comments below to match the format of the comments made by MSBA in its memorandum to you.

1. Costs:

1.a. The MSBA comments state that the M.S. 15.0412, Subd. 7 notice "... does not absolve the Department from the responsibility for its actions which create costs incurred through the implementation of its rules". Comments following this assertion seem to indicate that Rules 1.210, 1.220, 1.202I, and 1.214 through 1.217 are the "actions" of the Department which create costs.

Our general response to those comments is as follows: With one exception, each of the rules identified by MSBA is a rule that is derived directly from the words of the statute. It is the underlying statute itself, not the rules, that requires expenditures by school boards for compliance. The rules merely provide the necessary detailed guidance to supplement the command of the statute. (We will discuss each of the rules cited by MSBA in greater detail below.)

We acknowledged in the Notice of Hearing and at several points in the public hearing that there are costs associated with the implementation of the Act. Furthermore, we agree the costs may be a problem. However, the generation of that problem is a function of the Act and not of the rules.

MSBA asserts that it is unclear if pupil dismissal or employee termination data is investigative data. If such data fits the three criteria established by the Act and the rule, then it probably is investigative data if school districts so designate it.

j. 1.211 B.: The comments made by MSBA suggest that the intent of the rule is to limit the power of school districts over their agents. The comment fails to take into account the contents of Rule 1.212 A. 2. Under the provisions of the latter rule, the school board is clearly, within the rules, enabled to limit or extend necessary power to the Responsible Authority. The MSBA comments fail to take into account the fact that these rules not only have to provide guidance to Responsible Authorities subject to direction of a governing body, but also have to provide guidance to Responsible Authorities who do not report to such a body.

k. 1.211 C.: The word "prescribe" was used as a reflection of our understanding of the power of the Responsible Authority under the Act.

l. 1.213: The Responsible Authority's power to appoint designees is given by the statute. (See Minn. Stat. 15.1641 (a).) To fully comprehend the problem suggested by the comment, we need further elaboration by MSBA relative to the effect of this rule on joint powers agreements. We fail to see how this rule affects joint powers agreements at all. Furthermore, given the Act's definition of "statewide system", it may very well be that joint powers agreement organizations are in and of themselves entities.

m. 1.215: Although we are sympathetic to MSBA's comment that there may be files that are subject to both sets of standards, i.e., the pre-1975 and post 1975 determinations, we call your attention to Minn. Stat., Section 15.1641 (c). The requirement to make these determinations is a mandate of the Act, not a duty created by the proposed rules.

Paragraph C.: The liability questioned by MSBA may very well be present. However, it appears to us that liability would stem from the entity's violation of Minn. Stat., Sections 15.165, Subdivision 2, or 15.1641 (b) and (c). The rule merely proposes a method whereby the Responsible Authority can perform tasks that will assist him/her in complying with these requirements of the Act.

Paragraph E: The MSBA comment seems to be saying "How can school districts be charged with knowledge of laws, both federal and state, that have a direct effect on the operations of school districts?" We find it difficult to

MSBA appears to have omitted a key consideration in viewing the projected costs. As was discussed at the rule hearing, one of the key elements that will diminish costs is the extent of current compliance by a given agency with the statute. In the case of school districts, this includes compliance with the Family Education Rights and Privacy Act of 1974 (emphasis added) and the rules promulgated thereunder in 1975. Many of the activities contemplated by the proposed rules will assist agencies in their compliance with M.S. 15.165, a section of the Act on which rules may not be directly written. This section of the Act has placed positive duties on school districts since 1975. The Department of Administration will not, and reasonably should not, take responsibility for the fact that many school districts have not chosen to comply with either the state or federal acts. We suggest that this lack of compliance may, in terms of either defeats in litigation or loss of federal funding (the punishment for non-compliance with the federal act and rules) prove far more costly to school districts than implementation of these rules.

Our response to the specific rules as mentioned by the MSBA comments is as follows:

Rule 1.210: As we stated at the hearing, direct and express authority for this rule is not presented by the Privacy Act itself. However, again as we stated at the hearing, it is clear to us that it is virtually impossible for an agency to comply with almost every section of the Privacy Act unless it has classified all of the data it maintains. (Also, see the discussion of this rule in the Statement of Need and Reasonableness.)

Rule 1.220: This is the brief rule dealing with emergency classification. Its only purpose, as demonstrated by the rule itself and the Statement of Need, is to provide some of the detailed guidance that the statute does not provide. We fail to see how this rule generates costs to school districts. Preparing an application for emergency classification of data is an optional feature of the Act. Nothing in the rule requires a school district to do anything unless it exercises that option.

Rule 1.202, I: This rule is the definition of federal law. Its sole purpose is to provide guidance to responsible authorities as to what in "federal law" they can rely on if they want to withhold data from the public by asserting certain data is private or confidential. We fail to see, given the plain words of the statute, how defining this term causes this Department to create costs to school districts.

Rule 1.214: We agree that this rule may generate costs. However, we call your attention and the attention of MSBA to the requirements of Minn. Stat., Section 15.163. Except for requiring citation for authority to withhold data and identification of designees, the rule is written exactly to the requirements of the Act. This is a requirement of the statute, not a creation of the Department of Administration.

Rule 1.215: We agree that this rule may generate costs. We again call your attention to Minn. Stat., Section 15.1642. The rule merely provides administrative details and a reasonable interpretation of that section of the statute. This is a requirement of the statute and not a creation of the Department of Administration.

The same comments that we have made for Rule 1.214 and 1.215 are also apropos of Rules 1.216 and 1.217. MSBA contends that the Department created costs with each of these rules. However, MSBA fails to note that the statutory sections to which these rules correspond impose duties on agencies by using the mandatory "shall" language and not the permissive "may". We find it difficult to see, given this mandatory language, how the Department has created obligations for school districts.

1.b. As with many of the other MSBA comments, it is our response that the comment goes to the Act itself and not to the rules. It is obviously impossible for this Department to appropriate funds. MSBA's dispute in this area is with the Legislature, not with the Department of Administration.

2..& 3. The general comments of MSBA corresponding to these numbers state that the rules do not provide "standards and criteria for discretionary actions by responsible authorities." However, the specific comments made under the enumerated sections do not appear to provide specifics as to which rules do not provide standards and criteria. The comments by MSBA ignore the major thrust of the rules which provide such "standards and criteria." The

Department's specific response to those paragraphs discussed under points 2. and 3. of the MSBA comments is as follows:

The concern evidenced by MSBA's comments in the first paragraph under 2. and 3. seems to be with the "substantially provides" language in certain definitions and with the "discretion" of responsible authorities to classify data. It is clear from a reading of the statute that in actuality responsible authorities have little or no discretion in classifying data. Responsible authorities are required to make a determination based on a reading of Minnesota Statutes and federal law as to whether certain data under their custody is anything other than public. The sole purpose of the "substantially provides" language is to allow responsible authorities to make a proper reading of old state statutes and federal law where those references do not use the specialized definitions of the terms private, public and confidential that are in use in Minnesota.

It is the opinion of the Department that "substantially provides" is not vague. The full text of the definitions provides the Responsible Authority with necessary guidance in evaluating authority to withhold data from the public as required by Minnesota law. We completely fail to see how use of this language makes these rules unreasonable as suggested by the MSBA comments. The assertion by MSBA that "substantially provides" is the only guidance provided to Responsible Authorities is not correct. Each of the definitions the MSBA comments identify contain substantial guidance, within the statutory limits. Again, it appears to us that MSBA's argument goes to the statute and not to the Rules.

MSBA's comments on the definition of federal law are puzzling to us. Generally, public agencies want the most expansive possible definition of federal law in this area because it affords them the opportunity to find some authority somewhere to withhold data from the public. As a matter of fact, the definition as proposed was adopted at the urging of public agencies when we solicited comments some months ago. (See the comments by Hennepin County submitted by us to you.) Some of those public agencies urged us to include federal <u>agency decisions</u> as another part of federal law. It is not the intent of the proposed rule to

say that an Oregon federal court decision is binding on a Minnesota School district. It is the intent of the rule to provide Responsible Authorities with the option of using an Oregon court decision as a basis for the classification of data as not public. If school districts do not want that possiblity of wider discretion, we will be happy to re-examine this rule. However, to do so will then generate negative comments from other public bodies in this state who want the more expansive definition.

Although the general title of MSBA's comments 3. and 4. is referred to as lack of standards and criteria, the last four paragraphs of comments under 3. and 4. appear to be a criticism of the Department of Administration for not having enough staff and funding to provide technical assistance to school districts. We fail to see how this criticism relates to lack of standards and criteria in the Proposed Rules. Furthermore, we hasten to point out that the Data Privacy Unit has provided significant technical assistance to school districts over the last four years. Although we do operate within staff and budgetary limitations, as we are required by law to do, we can think of no occasion in the last four years when we have not responded to a request for assistance from a school district. We would add that if MSBA feels so strongly about our lack of funding and staff, we urge them to support our appropriation request in the next legislature. We have consistently, when allowed to do so by the Governor, asked for more money than we have received. The bulk of expenditures that have been cut out of our budgetary requests are those funds that we would have allocated to staff to provide more technical assistance and training to agencies such as school districts.

4.a. We will consider changing the wording of 1.202 D.1.a. as suggested.

b. It is clearly the intent of the proposed definition of "individual" to take the position that "privacy rights" do not survive the death of a human being. (See the discussion of this point in the Statement of Need.)

c. 1.203 A.1.b.: The rule adopts the reasonable time standard for a number of reasons. Time limits in number of days have been considered by the legislature in reviewing amendments to Minn. Stat., Section 15.17. One reason such limits were not adopted was that no consensus or compromise emerged as to what the number of days should be.

The MSBA comment refers to a federal law that prescribes a timetable. However, that law is not identified. If the reference is to the federal data privacy or freedom of information acts, there is no comparability with this time question in the Minnesota Act. Among other things, those acts require the establishment of privacy and freedom of information compliance units in each federal agency. It is a priority task of such units to respond to requests for information. Given the broad range of data covered by the Minnesota Act, including data which may be 25-50 years old and maintained in warehouse type facilities, it appears to us that reasonable time is the appropriate standard.

d. We will make the changes suggested to the rules noted in the MSBA comment.

e. 1.205 B. 2. a.: This proposed rule was lifted verbatim from the HEW rules implementing the Family Educational Rights and Privacy Act of 1974 (FERPA). This rule was adopted by HEW at the urging of educators. As you may remember, this particular rule was supported by public testimony at the Hearing.

f. As the MSBA comments point out, this rule covers a subject that is the express subject of Minn. Stat. 15.162, Subd. 4. However, the MSBA comments fail to point out that this duty of the Responsible Authority is stated as a mandatory "shall" in the Act itself.

(1) Although the required "determinations may be beyond the skill and training of the responsible authority", it is the Act that requires the determination to be made by him/her. There is nothing in the rule that precludes the Responsible Authority from consulting with a doctor, lawyer, etc. to assist the determination.

(2) The intent of the criterion set out in C. 2. a. 5. is clear. Contrary to MSBA's suggestion that this criterion is a "trap", it is the clear intent of the rule, when set in the context of FERPA and the federal rules, to tell the responsible authority in a school district that he/she cannot deny parental access to "education records" as defined by FERPA. Contrary to MSBA's assertions, there are numerous exceptions under the federal law. FERPA and its rules only regulate "educational records" as defined. There are several types of data on individuals subject to the provisions of the state act which are not the subject of FERPA. These include such data

as records on students which are "only in the possession of the maker thereof." (Quoting an exception from the FERPA rules.) A review of the definition of educational records in FERPA will reveal to you the numerous exceptions. The entire thrust of 1.205 C. is pointed toward "data on individuals" which are not "educational" records for FERPA purposes.

(3) The references in 1.205C. to Minn. Stat., Sections 144.341 to 144.347 were added to the proposed rules after we were urged to do so by public bodies during the period when we solicited comments before finalizing the rules. Again, there is nothing in the rule that precludes the Responsible Authority from seeking professional advice from others in making this judgement.

g. 1.206 B. 1. c.: MSBA's comment asserts that this rule is not consistent with 1.204 B. 2. a. and b. It is not intended to be consistent. Rule 1.206 is concerned with access to confidential data. Fule 1.204 is concerned with access to private data. It is obvious that different standards whould be applied because the data in question commands different levels and types of protection.

h. We agree with the MSBA comment that school districts may have elements of data that are equivalent to arrest information. As discussed in the Statement of Need and at the public hearing, that is exactly why we have proposed the arrest information definition. Although MSBA asserts that it is unclear what school districts "may do with this information", it is very clear that this type of information is subject to all of the rules pertaining to data on individuals.

i. 1.208 B.: As we stated at the hearing and as discussed in the Statement of Need, the handling of investigative data starts from the premise that Responsible Authorities have the discretion to designate data as investigative, subject to the limitations of the Act. The rules on this point deal with the exercise of that discretion. However, as with any rules and for that matter any statute, the rules proceed from the premise that public administrators will act reasonably. Therefore, we find it difficult to believe that public school administrators, particularly given the limits on this discretion as proposed by the rules, would act so unreasonably as to designate <u>all</u> data held by them as investigative data.

respond to such a comment. The comment goes on to suggest that the Commissioner's approval must be given to initiate any new purpose or use of private or confidential data. As we said repeatedly at the hearing, these rules are written in very tight conjunction with the statutes. A clear reading of the rule in question and the applicable section of the Act makes it clear that the Commissioner's approval is only necessary when there is not a new mandate or when informed consent cannot be gained. The Commissioner's approval is the exception, not the rule. In the four years of data privacy legislation, the Commissioner has been asked to give such approval five times. If, as the comment says, federal law requires the new purpose, it is clear both under the Act and the rule, the Responsible Authority initiates the new purpose. No further approval is necessary.

We are sure that conflicting opinions by parents about their children are matters that school districts confront every day. We do not find it reasonable to write a rule to deal with such conflicts when the proposed rules are based only in the Data Privacy Act. We suggest that the guidance provided by Rule 1.205 B. 2. a. is sufficient for data privacy purposes.

n. The general thrust of the four paragraphs of comment made by MSBA in this section seems again to be directed at the statute itself and not at the rules. The statute requires the Responsible Authority to make a great number of decisions and determinations. As with many other issues of modern public administration, this may indeed require legal guidance. However, we fail to see how the guidance provided by the rules exacerbates that problem. As a matter of fact, there were comments made at the public hearing which applauded the proposed rules for eliminating many of the common uncertainties and questions.

5.a. If the so-called "gap" theroy is a viable theory of statutory construction, then assessor's field cards are not official records within the meaning of Minn. Stat., Section 15.17 and therefore they are not accessible to the public. However, as we pointed out at the hearing, we are faced with the following dilemmas in dealing with public data:

(a) The Kottschade case is ten years old and was decided on very narrow grounds.

(b) The intervening ten years has seen an explosion in the concepts of freedom of information and openness in government.

(c) Although the subject of Minn. Stat. 15.17 is official records, the subject of the privacy act is all data on individuals maintained by the state and its political subdivisions.

(d) The last sentence of Minn. Stat., Section 15.162, Subdivision 3 states very clearly: "Data on individuals are classified as public, private or confidential."

(e) Over and over public administrators have told us they cannot implement the privacy law because they cannot establish, given the definitions of public data in the statute, what data is public within their agencies.

We leave to you, given those factors among others, whether the definition of public data on individuals as proposed by the Department is necessary and reasonable.

b. We think the previous comments on "federal law" are a sufficient response.

c. 1.218: This rule receives extensive treatment in the Statement of Need. We believe it to be a reasonable interpretation of the statute given the provisions of the Statutory Construction Act, Administrative Procedures Act and the Privacy Act. We further point out, as MSBA has pointed out several times, that the Data Privacy Unit does operate on a severely limited budget. Unless we can bill back costs of contested case proceedings, we will be unable to provide the administrative appeal that is mandated by the statute. (See Minn. Stat. Section 15.165, Subdivision 4.)

Given the tone of MSBA's comments on this point, we would also point out that the Commissioner must make determinations if it is appropriate to convene a contested case proceeding. We seriously doubt he would do so in the instance of a "frivolous or unwarranted" appeal. We would be happy to investigate the possiblities of adding words to that effect to the proposed rule.

6. The MSBA comment speaks to differences between the state act and the federal act. We have previously pointed out in other responses that it is our position that FERPA clearly states that denial of parental access cannot extend to data contained in "educational records." This requirement of FERPA is one of the reasons we constructed the rule on denial of parental access as we have. We are very aware of the requirements of FERPA and the rules promulgated thereunder.

Our "expertise" with FERPA stems from assisting school districts and other educational institutions with suggestions for administrative methods of compliance with FERPA and the state act. We know that proceedings have been developed by school districts that are in basic compliance with both FERPA and the state act. We regularly encourage exportation of these procedures as a cost reduction method. Given that background, we made a conscious attempt, and we think a successful one, to harmonize the proposed rules with FERPA. In the past there were direct conflicts between FERPA and the state act. We have worked with the legislature to eliminate those conflicts. If MSBA knows of any remaining direct conflicts, we would appreciate knowing about them.

In response to MSBA's assertion that there is confusion about "desk copy information on students", we assert there is no confusion. It is clear that such information is one of the exceptions to FERPA. Such information is not an "educational record" within FERPA. Clearly, it is data on individuals subject to the state act. Furthermore, it is clearly data that must be classified by a school district. To date, we have received applications from school districts, under Minn. Stat., Section 15.1642, to classify exactly that kind of information as private or confidential. The Commissioner has approved classifications of private.

Again, we fail to see how the rule's definition of federal law complicates "the dovetailing of the two laws." As stated earlier, we know of no direct conflicts. As a matter of fact, a number of school districts are maintaining that the provisions of FERPA "substantially provide" that educational records are private data within the meaning of the Act. We agree that this is a reasonable interpretation of FERPA and the state act, particularly in light of the proposed rules.

7. In response to this comment by MSBA, we would request that they point out to us in greater detail those protions of the Privacy Act that expressly provide this Department with responsibilities "beyond our budgetary limitations". We have presented our case to the legislature on enforcement powers in every legislative session since 1974. They have not deemed it proper, as yet, to either extend those powers or to increase our appropriations. They have, however, made it very clear that we should promulgate rules forthwith. (See the Report of the Joint House-Senate Privacy Study Commission, December, 1976.) Again, we hasten to point out that we provide assistance to school districts on a continuing

basis. As stated earlier, we know of no occasion when we have turned down a request for assistance from a school district. As with many comments of MSBA, we find this comment to be directed to the statute itself and not to the rules as proposed by the Department. Hopefully, MSBA is aware of our continuing efforts in the Legislature to evolve successful privacy legislation. We fully intend to continue those efforts in the coming session and urge MSBA to make its concerns with the Privacy Act known to the Legislature.

DAG:mm

cc: Richard L. Brubacher
Sheila Fishman
Daniel Magraw
W. A. Wettergren

STATE OF MINNESOTA
OFFICE OF THE ATTORNEY GENERAL
ST. PAUL 55155

WARREN SPANNAUS
ATTORNEY GENERAL

TELEPHONE
(612) 296-6196

November 20, 1978

Steve Mihalchick
Hearing Examiner
Office of Hearing Examiners
1745 University Avenue
Saint Paul, Minnesota

Re: Proposed Rules - Data Privacy

Dear Mr. Mihalchick:

This letter is written on behalf of the Department of Administration in the above-captioned matter and is in response to the comments of the Minneapolis Star & Tribune regarding the proper interpretation of "legal action." The proposed rules which are affected by the comments are sections 1.208(B)(1)(d) and (e); 1.208 (B)(2)(f) and (g) and 1.208(B)(3)(c) and (d). The agency's comments are as follows:

The Minneapolis Star & Tribune has pointed out that Minn. Stat. § 645.45 defines "action" as "any proceeding in any court of this state." The proposed rules include the quasi-judicial procedures of license revocation and arbitration proceedings as well as court procedures in its rules implementing section 15.162, subd. 2a. The newspaper points out that because the questioned activities are not in any court, the rules go beyond the statute. However, section 15.162 provides, in part, that certain data is classified if it is

> . . . part of an active investigation undertaken for the purpose of the commencement of a legal action.

In this regard, both an arbitration and a license revocation hearing can be confirmed or appealed to a court. For example, Minn. Stat. § 325.62 which provides for an appeal de novo of a license revocation

proceeding to a District Court; Minn. Stat. § 80A.24 provides that orders of the Commissioner are subject to judicial review pursuant to chapter 15, and Minn. Stat. §§ 572.18, 572.19 and 572.20 provide for application to a court in regard to an arbitration award. Because these administrative or arbitration procedures can be followed by a legal action (as the Minneapolis Star & Tribune urges that it be defined) the inclusions of these procedures into the rules is logical, and certainly proper.

Even if there were no provision for a court action, section 645.45 provides that the definitions contained therein are not controlling if "the context in which the word is used indicates otherwise." In the present situation, section 15.162, subd. 2a provides that data is confidential if it is "collected by a Civil . . . investigative agency . . . ." With few exceptions, the Civil investigative agencies of the State have authority to resolve its investigations through quasi-judicial procedures. This authority results in numerous administrative actions which are frequently concluded without resort to the courts. These procedures, which are relatively new, are outlined in the Administrative Procedure Act (Chapter 15). Because the APA was used frequently by the state agencies at the time of the passage of the Data Privacy Act, it is clear that under the laws governing the interpretation of statutes and under the express exclusion of section 645.45, section 15.162, subd. 2a should be given a broad reading to include the purpose of a quasi-judicial proceeding. Similarly, the legislature has provided arbitration procedures in Chapter 572. These too are enforceable by courts and are quasi-judicial in nature.

The Minneapolis Star & Tribune cites Har Mar, Inc. v. Thorsen and Throshov, Inc. and Muirhead v. Johnson in support of its position that the proposed rules have gone beyond the terms of the statute. The Har Mar court was specifically concerned with the statute of limitations and the likelihood of the legislature's including a "limitation" in the arbitration statutes. The Muirhead case concerns the rules of civil procedure. The present matter is clearly distinguishable. It involves the nature of arbitration or administrative hearings as quasi-judicial proceedings.

Because the legislature has used broad language and because the Commissioner of Administration has the authority "to implement the enforcement and administration" of the Data Privacy Law, it is clear that the proposed rules interpret section 15.162, subd. 2a properly and reasonably.

Respectfully submitted,

SHEILA S. FISHMAN
Special Assistant
Attorney General

Attorney for
Department of Administration

SSF/bw

ADMIN 1000 (Rev. 1/78)

STATE OF M ESOTA

DEPARTMENT OF ADMINISTRATION

Office Memorandum

TO : Steve Mihalchick
Hearing Examiners Office

DATE: November 20, 1978

FROM : Don Gemberling
Data Privacy Unit

PHONE: 296-6733

SUBJECT: Response to Comments Made by Rodgers Adams on Behalf of the Minneapolis Star Tribune

General: At several points, the comments made by Mr. Adams speak abstractly of the need to define legal terms according to their "legal meanings". Case and statutes are cited to support that comment. However, the comment fails to address the fact many of the terms referred to have no generally accepted and clearly "established legal meanings." Although the terms may be defined within certain cases, that is not dispositive of whether the terms are defined sufficiently for purposes of "implementing the enforcement and administration" of the data privacy act.

Page 3, Comment on 1.202B.: As other comments you have received, the School Boards Association and the Department of Economic Security demonstrate, the rules concerned with the question of the type of agency maintaining "arrest information" is clearly not a "specious" issue as suggested by the comment. We call your attention to the Statement of Need's discussion of this issue, particularly the context of the legislative deliberation which produced the arrest information definition in the Act. We only wish that all of the problems associated with "arrest information" were clearly handled by the statute as the comment suggests.

The Attorney General's opinion on this point and continued disagreement between the media and police agencies clearly demonstrate that the statute does not provide clear guidance on this point. Where such confusion reigns, it is clear that a rule eliminating that confusion is appropriate.

Pages 3 and 4, Comments on 1.202 D., 1.202 E. 1., and 1.202 E. 2. b.: The word "substantially" was placed in the Rules to deal with the older statutes and clearly applicable provisions of federal law that must be construed in light of the data privacy act's definitions of private and confidential. To use the word "expressly", as suggested by Mr. Adams' comment, would further complicate a problem we know to exist and would not provide reasonable and necessary guidance.

Page 4, Comments on 1.202 I.: As other comments you receive indicate, agencies want the broadest possible definition of federal law. Media representatives want the narrowest definition. We believe the proposed rule presents a reasonable compromise to those totally antithetical desires.

Page 5, Comment on 1.202 M.: The comment fails to take into account the fact that the rule is definitional in nature and must be read in light of the specific requirements concerning summary data that are set out in Rule 1.209. We believe Rule 1.209 addresses the concerns raised by the comment.

Page 5, Comment on 1.203: We fail to understand the comment's assertion that the rule has some effect on "third parties". It is clear under the proposed rule that public data is accessible to anyone. As we stated at the public hearing, we are aware of the problems associated with the rule's dealing with public data. However, we fail to see how we can comply with the statutory requirement of Minn. Stat. Section 15.1671 without addressing the subject of public data. Without a clear understanding of what public data is, agencies will never be able to implement the privacy act.

Page 6, Comment on 1.204 A. 4.: The comment makes reference to "informed consent" as the authority for an individual to have an agency disseminate data about him or her. This comment reflects a misreading of the act. "Informed consent" only comes into play when the agency seeks to initiate a new purpose or make a new use of private or confidential data previously collected from a data subject. (See Minn. Stat. 15.1641 (c)). The rule deals with assuming the individual's ability to direct the dissemination of private data about himself or herself. Problems with this situation are common. They arise from the act, but are not expressly handled by the statute.

Page 6 and 7, Comments on Rule 1.207: The comments fail to take into account the necessity to give some construction to the words "reasonable contemporaneous" that appear in the statute. We continue to believe, given the legislative context and the language of the Title 28 rules as originally proposed, that this is a reasonable construction.

Page 7, Comment on 1.207. C.: We continue to believe this rule is reasonable, particularly in light of the problems with the statute's handling of the concept of "investigative data", the public's interest in crime events, and the realities of the current relationship between the media and police agencies. The rule as proposed is an attempt to balance those factors and interests. However, given the strong media reaction to the proposed rule, we will consider modifying it or if necessary deleting it completely.

Page 7, Comment on 1.207. D.: We disagree with the comment's assertion that the proposed rule is not authorized by the statute. Juvenile data is data on individuals within the meaning of the act. The Commissioner is authorized to promulgate rules to implement the "enforcement and administration" of an act whose express subject is data on individuals. We know that there are specific problems with the administration of juvenile data. The media comment suggests that we should ignore those problems in rules whose very objective is to cure such problems. Furthermore, nothing in these rules is intended to change the discretion afforded to juvenile judges by Minn. Stat. Section 260.161 to administer juvenile data on individuals within the latter statute.

Page 8, 9 and 10, Comments on 1.208: Sheila Fishman is preparing responses to Mr. Adams' comments. Those responses will be submitted to you under separate cover.

Page 10, Comment on 1.220 D.: A clear reading of the proposed rule reveals that it does not change the act's intent to classify data covered by the application for the limited time set out in the act upon filing. The rule merely clarifies what actually constitutes "filing" of an application, both for purposes of the act and for the Department's processing of the application. It is the position of the Department that an application would not enjoy the 20 or 30 day temporary classification of data until the application is properly filed as described by the proposed rule.

DAG/rm

Mpls Star Tribune

protects the identity of the juveniles and serves the interest of both the juvenile and the public. Cf., In the Matter of T.L.K. and R.L.K., ___ Minn. ___, 269 N.W. 2d. 367 (1978).

Sec. 1.208 B. 1. d. and e., B. 2. f. and g., and B. 3. c. and d.: References to all arbitration and licensing procedures is an unreasonable and over-broad interpretation of ``legal action.'' The term should be limited to those situations which are formally initiated in a court of law, and should exclude actions that are initiated before non-judicial or quasi-judicial agencies, whether or not they may be eventually appealed to a court of law.

Although neither Minn. Stat. 15.162 through 15.169 nor the Proposed Rules define the term ``legal action,'' other Minnesota statutory law and Minnesota Supreme Court decisions suggest license revocation proceedings before administrative bodies and arbitration proceedings are not ``legal actions,'' and thus are not covered by the term ``investigative data.''

See. Minn. Stat. 645.45, which defines ``action'' as ``any proceeding in any court of this state.'' Section 645 is the chapter of statutory construction.

See also, the Har Mar, Inc. v. Thorsen and Throshov, Inc., 302 Minn. 149, 218 N.W. 2d. 751 (1974). The Minnesota Supreme Court held that arbitration proceedings are not ``actions'' subject to the 6-year statute of limitations for commencing ``actions'' on contracts. The Court said arbitration proceedings are intended to discourage litigation, and thus are nonjudicial in nature.

See also, Muirhead v. Johnson, 232 Minn. 408, 46 N.W. 2d. 502 (1951). The Minnesota Supreme Court said an ``action'' is

``the prosecution in a court of justice of some demand or assertion of right by one person against another.'' (Emphasis added.)

Sec. 1.208 B. 1. c.: The reference to judicial entities should make clear that this section applies to them only in their roles as investigative agencies, as in the case of pre-sentence investigations. As we said in our oral presentation, the provisions regarding investigative data should not apply in situations where the data is transferred from the investigating agency to another agency in what would otherwise be a public act, as in the case of information included in requests for subpoenas, arrest warrants and search warrants, which now become public records when included in the court record. See attached Prepared Remarks, page 4.

Sec. 1.208 B. 2. d.: The provision regarding civil answers goes beyond the scope of the statute, which applies only to data ``collected. . .as part of an active investigation undertaken for the purpose of the commencement of a legal action.'' (Minn. Stat. 15.162, subd. 2a. (b).) A civil answer presumes that a legal action has already been commenced. (Rule 3.01, Minn. R. Civ. P.)

Sec. 1.208 B. 2. e.: The reference to ``maintaining or prosecuting a civil or criminal action'' goes beyond the scope of the statute, which refers to information gathered prior to the ``commencement of a legal action.'' In other words, once an action has commenced, there should be no such term as ``investigative data.'' The provision should be deleted.

Sec. 1.208 B. 3.: In our oral comments (see attached Prepared Remarks, pages one and three), we have already objected to the way these rules confuse ``active investigation,'' a concept in the law (Minn. Stat. 15.162. subd. 2a), with ``active data,'' a concept not found in the law. All the criteria listed under 1.208 B. 3. must be redrafted to accurately reflect the statutory concept of ``active investigation.''

Page 360

Sec. 1.220 D.: This extension of time is not authorized by statute. Minn. Stat. 15.1642 sets forth definite time limits for the processing of applications for emergency classification. To adopt the unusual, flexible definition of ``filed,'' as the Proposed Rules do, is clearly contrary to the statute's stress on prompt actior and rigid time limits. A reasonable defition of the term ``filed'' is the point at which the Commissioner of Administration is first notified of the request. That definition is also more in keeping with another provision of the statute than is the definition in the Proposed Rules. Minn. Stat. 15.1642, subd. 1, protect the privacy of information during the processing of an application for emergency classification by providing that it is automatically and temporarily classified at the point the request is filed. This implies a definition of filing that takes effect at the earliest possible date. The definition in the Proposed Rules would leave the data unprotected for 30 days, an effect clearly contrary to statute.

Oct 31

Public Hearing — Notes

? 5 Working Days — 20

→ Monday, November 20 - Record Closes

Procedures

Aug 21
Open File
Exhibit A

Oct 5
✓ Order - B ✓
✓ Aff. Mailing C ✓
✓ Notice as mailed D ✓
Cover letter
Register
✓ Aff of Receipt E ✓
✓ Sec of St. - F
Aff - reviewed G
✓ Names of Witnesses H
✓ Statt of Need I ✓
✓ Mat received J
J. Fitz. - K - rec Oct 13
Public Comments
Errata - L

Errata

Explanation
No substantial change

Dan Maguire
Introduced Rules

Comments

Rodgers Adams
Asst to Edit of Gov - Tribune

Investigative Data
Definition - when begin, when end -

Concerned that it might involve any fact gathering

Suggests: Preliminary fact finding
Something non-routine

Subsequent decision → previous facts become class. as conf.

Define beginning : Need rule -

When end? Rule is reasonable!
Rules change active invest. → active data.

Rules → need clarification (pt: do not go far enough)

Rules could cover search warrants and subpoenas under Judicial Agencies (rather than pre-sentence type investigations).

Suggestions -
exempt clause

Arrest info. - reasonably contemporaneous
Disagree
Rules: timeliness of request
Law: does not suggest timeliness
AG Opinion

Public Data - in rules
Criteria useful
reasonable
Public accessibility: cost
Computers - hard to get!
15.17 - doesn't authorize
Unreasonable to charge.
Contradictory to spirit of 15.17

Comments submitted -

Charles Schaffer -
Comments submitted - read

Richard Cottrell
Ms Dept of Personnel
Pts -
1. Rules too complex
2. Charge: Dept of Pers. cannot charge - Costs not recoverable.
Minimal - 2

Under what basis?

Comment here: Rules don't encompass all of 15.17

Financial Impact -
Stat is so low as to be misleading -

Comment: Implement rules or statute?

David Laughlin

Cert. Record Teacher - Professional Researcher -
Adequate -

Needs more good words
"easily accessible
"Free, easy, convenient & comprehensive access"

Good procedures should be in writing -
"Clear public written procedures"

A 1-b - oral or written request

C disagree - no fees for public data.
Does not tell enough
May better than shall

Need rules on cert. Fed or uncertified copies.

John ~~Beal~~ Diehl
Nat'l Hospitals
Mu Hosp. Assoc. } appearing for:

180 Hosp. - 1/3 of which are public

Medical Records - dist. from other records maintained by govt. -

HH. 335 Medical Records

Suggest Comment from Admin. - Rules cannot classify

Rules: new requirements unnecessary.
30 new tasks of R/A
Comment: Stat requires 25 (?)
Costs: permissive

Releases: notarized -
would delay 3rd party
Delays - increase costs

Conf. Data - 1.202 (1)(E)(11)(d)
into clause (D) for subd (c)

Pt. - 144 establishes guidelines
+: can unless released
Wants 144 to classify
or acknowledge

Comment: pigeonholes problems -
emergency class. or stat.

Notarized requirement - Should be taken out?

ment?

Q- emergency?

Records of Minors
~~Access to~~ re
Stat problem
144.335 - Costs discr. in
provider -

Considr. emergencies re
21.205 (c) (1)
Reference to 144.335

R.A. - who has responsibility to
determine.

Burden under law for rules -
Costs - Admin Agencies
burden to show reasonable.

Ralph Marlett
Insurance companies representative

Notarization
Increases expense & problems
Does not help significantly

Suggestion: Reas. efforts made for
det.

comment out?

Fire Marshalls - reluctant to release
info. - wants amendment to en-
courage release
Comment: Have no authority to permit release.

Dale Swanson
Rep. MESP Assoc
(Minn Elementary School Principals)

Procedural Defects
Teachers go to arbitration
to contest accuracy & completeness of data

1.215 – Procedural Review
Remedies not described
Supplement Record ?
Correct & expunge ?

Records of Minors
1.205 D 2 A

Statement of Need –

Agency Comments & Presentation:

Scope & Purpose

Non profit
Non

Public Data –

Duke Addicks
Public data → goes beyond statute – goes too far.

Preserves existing muddle!

Our comment?
Cannot say all that is not private or conf. is public.

Pat Hirl
* R/A –
"employee or officer"

Comment: Gerbig: had no objection – should confirm in writing

Davis –

Comments – Attics – Hirl

Access to Public Data 1.203
A-1-c may –
A-1-b – "reasonable" – better to say "prompt"

Good deal of support for may – ||

DO we agree?

Pat Hirl: Written refusal? –

144.335 – Rules Harmonious w/ Stat. –
No Conflicts

Joel Turney

Waiver of access to private info. -
Fed rules - ?
FERPA

(Presumably can be done under legal theories?)
Should not require rules to accomplish.

Arrest Info.

reas. contemp. → duration of time

You on read needed help from us

Comment: need explanation of C (1.207)
Invest. Data = Conf. - but
agencies can define what is
investigative data

Ceases to be invest. data?
Need for doing this clear; where is authority?
- Investigative -

Ask for written suggestions To add.

Technical legal procedures

1.209

→ delegation to "a person" —
limited or broad
Restrictions on purposes?

Duties of Responsible Authority

Classification
Past budget time for cities

Lead time may help –

Comment: Should we agree? 210 – Compromise –
Require class of private + conf only

Comment: Why rules have not said all data not private or conf. is public.

Suggestion for alternative from Pat Hitch + Duley –:
Give statut. justifying refusal
for each document

1.215 – Duke:
Use ~~only if~~ – classify only
Comment: Shall we concede this point? if need. Don't classify everything.
This is esp. imp. for old material.
Q – Can one legally go back & classify – 215(B)

1.214 – Stored Data

STATE OF MINNESOTA

DEPARTMENT OF ADMINISTRATION

IN THE MATTER OF THE PROPOSED ADOPTION
OF RULES OF THE DEPARTMENT OF ADMINISTRATION
GOVERNING ENFORCEMENT AND ADMINISTRATION OF
THE MINNESOTA "DATA PRIVACY ACT"

ORDER FOR HEARING

IT IS HEREBY ORDERED that a public hearing on the above-captioned rules be held in Room 83, State Office Building, St. Paul, Minnesota on October 31, 1978 commencing at 9:00 a.m. and continuing until all persons have had an opportunity to be heard.

IT IS FURTHER ORDERED that a Notice of Hearing be mailed to all persons or representatives of association or other interested groups who have registered their names with the Secretary of State for that purpose.

IT IS FURTHER ORDERED THAT the Notice of Hearing be published in the State Register.

Richard L. Brubacher

Richard L. Brubacher
Commissioner

Date: August 21, 1978

STATE OF MINNESOTA

DEPARTMENT OF ADMINISTRATION

IN THE MATTER OF THE PROPOSED ADOPTION OF RULES OF THE DATA PRIVACY UNIT GOVERNING THE ENFORCEMENT AND ADMINISTRATION OF THE "MINNESOTA DATA PRIVACY ACT"

AFFIDAVIT OF RECEIPT OF THE SECRETARY OF STATE'S LIST

Brooke Manley, being duly sworn on oath deposes and says:

That she is an employee of the Data Privacy Unit of the Department of Administration, State of Minnesota.

That on the eighth day of September, she went to the Secretary of State's office for the State of Minnesota and requested a current list of all representatives of associations or other interested groups or persons who had registered their names with the Secretary of State for the purpose of obtaining notices of public hearings relating to the promulgation of rules pursuant to M.S. 15.0412.

That on the eighth day of September, in response to the above request, the Secretary of State provided her with such a list, a copy of which is attached hereto and incorporated by reference.

Further affiant sayeth not.
Subscribed and sworn to before me
this 22nd day of September, 1978.

Colleen T. Kisch
Dakota County, Minnesota

My Commission expires 4/24/85.

Brooke L. Manley
Brooke Manley
Data Privacy Unit
Department of Administration

COLLEEN T. KISCH
NOTARY PUBLIC—MINNESOTA
DAKOTA COUNTY
My Commission Expires April 24, 1985

STATE OF MINNESOTA

DEPARTMENT OF ADMINISTRATION

In the Matter of the Proposed Adoption of Rules of the Data Privacy Unit Governing the Enforcement and Administration of the "Minnesota Data Privacy Act"

CERTIFICATE OF DELIVERY OF THE SECRETARY OF STATE LIST

I hereby certify that the attached 529 labels 3 sheets constitute the complete list of persons, associations, and other interested groups who as of 9:30 o'clock A.M, this 8th day of September, 1978, have requested pursuant to M.S. 1974, 15.0412, that their names be placed on file with the Secretary of State for the purpose of receiving notice of public hearing on proposed rules on the subject captioned above.

Secretary of State

Joan Anderson Growe

By Donna Reet

STATE OF MINNESOTA

DEPARTMENT OF ADMINISTRATION

IN THE MATTER OF THE PROPOSED ADOPTION OF RULES OF THE DATA PRIVACY UNIT GOVERNING THE ENFORCEMENT AND ADMINISTRATION OF THE "MINNESOTA DATA PRIVACY ACT"

AFFIDAVIT OF MAILING

Rita Meyer, being duly sworn deposes and says:

That on the 14th day of September, 1978, at the city of St. Paul, County of Ramsey, State of Minnesota, she served the attached Memorandum, Notice of Hearing and Proposed Rules by depositing in the United States mail at said City of St. Paul, a true and correct copy thereof, properly enveloped with postage prepaid to all persons and associations at the addresses listed on the Certificate of the Secretary of State, to all cities at addresses provided by the League of Minnesota Cities, to all counties at addresses provided by the Association of Minnesota Counties, to all school districts at addresses provided by the Department of Education, to all state agencies and departments at addresses provided by the Department of Administration, to all community action agencies at addresses provided by the Department of Economic Security, to all mental health centers and developmental achievement centers at addresses provided by the Department of Public Welfare, to regional development commissions at addresses provided by the State Planning Agency, to district courts at addresses provided by the 1978 edition of the State of Minnesota Telephone Directory and by the County of Hennepin, to the University of Minnesota at an address provided by the University, and to county and municipal courts at addresses provided by the 1978 edition of the guide to Minnesota Elected Officials, published by the Secretary of State's office.

Rita Meyer
Department of Administration

Subscribed and sworn to before me
this 22nd day of September, 1978

Colleen T. Kisch
Dakota County, Minnesota
My Commission expires 4/24/85.

COLLEEN T. KISCH
NOTARY PUBLIC—MINNESOTA
DAKOTA COUNTY
My Commission Expires April 24, 19...

ADMIN 1000

STATE O NNESOTA

Office Memorandum

DEPARTMENT OF ADMINISTRATION

TO : STATE AGENCIES
POLITICAL SUBDIVISIONS
PERSONS REGISTERED WITH THE SECRETARY OF STATE PURSUANT TO MINN. STAT. § 15.0412
DIRECTORS OF "DAC'S" AND MENTAL HEALTH CENTERS
DIRECTORS OF COMMUNITY ACTION AGENCIES

DATE: SEPTEMBER 12, 1978

FROM : Richard L. Brubacher
RICHARD L. BRUBACHER
COMMISSIONER

PHONE: (612) 296-6733

SUBJECT: PROPOSED RULES GOVERNING DATA PRIVACY

This Department has drafted Proposed Rules concerning the "Data Privacy Act" as required by Minn. Stat. § 15.1671. A hearing to consider the adoption of these rules is scheduled for October 31, 1978, commencing at 9:00 a.m. in the State Office Building Auditorium, Room 83, on Wabasha Street between Aurora and Fuller, St. Paul, Minnesota.

Pursuant to § 15.1671, enclosed is a copy of the State Register of September 4, 1978, in which is printed the full text of the Notice of Hearing and of the Proposed Rules. The notice appears at page 346. The text of the Proposed Rules begins at page 347. Besides providing details concerning the hearing and other important information, the Notice describes procedures for written and oral comments concerning the Proposed Rules.

I advise each recipient of this memo to review the rules with care and in consultation with your agency's legal advisor since these rules have a direct effect on your activities and procedures.

Special Notice to Agencies Who have Contracts with Non-Profit Social Service Agencies: Certain nonprofit agencies under contract with your agency are subject to the provisions of the "Data Privacy Act" and to any legally adopted rules. Therefore, the Proposed Rules are of special interest to such agencies. Please inform those with whom your agency contracts of the date, time, and place of the hearing; of the nature and extent of the Proposed Rules; and of the availability of a copy of the Proposed Rules from this office.

Special Notice to Persons Registered with the Secretary of State: Minnesota Statutes § 15.0412, subd. 4 does not require that a copy of the Proposed Rules be sent to you. However, a copy is being provided so that you will be fully informed as to the content and extent of the Proposed rules.

RLB:mm

Enclosure

STATE OF MINNESOTA

DEPARTMENT OF ADMINISTRATION

IN THE MATTER OF THE PROPOSED ADOPTION OF RULES OF THE DATA PRIVACY UNIT GOVERNING THE ENFORCEMENT AND ADMINISTRATION OF THE "DATA PRIVACY ACT:

NAMES OF WITNESSES

Daniel B. Magraw, Assistant Commissioner, Department of Administration and Don Gemberling, Manager of the Data Privacy Unit will appear on behalf of the Department of Administration at a hearing to be held on October 31, 1978. They will testify regarding the need for and reasonableness of the proposed rules. The substance of their testimony is set forth in the Statement of Need submitted herewith.

Date: October 4, 1978

Donald A. Gemberling

Donald A. Gemberling, Manager
Data Privacy Unit
Department of Administration

STATE OF MINNESOTA

DEPARTMENT OF ADMINISTRATION

IN THE MATTER OF THE PROPOSED ADOPTION OF RULES OF THE DATA PRIVACY UNIT GOVERNING THE ENFORCEMENT AND ADMINISTRATION OF THE "MINNESOTA DATA PRIVACY ACT"

AFFIDAVIT CONCERNING REVIEW OF THE PROPOSED RULES BY THE INTERGOVERNMENTAL INFORMATION SYSTEMS ADVISORY COUNCIL

Donald A. Gemberling, being duly sworn on oath deposes and says:

That he is the manager of the data Privacy Unit of the Department of Administration, State of Minnesota.

That commencing on October 6, 1977 a series of meetings were held with members of the Intergovernmental Information Systems Advisory Council.

That those meetings were held for the purpose of receiving the advice concerning the draft rules as required by Minnesota Statutes Section 15.1671.

That on November 23, 1977, I received from Mr. Jerome J. Segal, Chairman of the Council's Records Management Committee, a letter, a copy of which is attached hereto and incorporated by reference, which states that the Council had provided the advice as required by Minnesota Statutes Section 15.1671.

Donald A. Gemberling

Donald A. Gemberling
Manager, Data Privacy Unit
Department of Administration

Subscribed and sworn to before me this 3rd day of October, 1978.

Colleen T. Kisch

Dakota County, Minnesota
My Commission expires 4/24/85.



November 21, 1977

RECEIVED
NOV 2 3 1977
DATA PRIVACY

Mr. Donald Gemberling
Manager
Data Privacy Unit
Department of Administration
Room 110
Nalpak Building
Saint Paul, Minnesota 55101

Dear Mr. Gemberling:

On behalf of the State Department of Administration your office has prepared a draft of regulations applicable to Minnesota Statutes, §15.62 through §15.169. Intergovernmental Information Services Advisory Council (IISAC) was requested to review the draft regulations and advise the Commissioner of Administration pursuant to the legislative mandate contained in M. S. §15.1671. IISAC referred the request to its committee on records management, of which I am the chairman. Starting in October the committee met three times to discuss the draft. Copies of the draft were referred to all members of IISAC and comments were invited. Our committee originally estimated a need for at least 90 days for review, and possibly 180 days. Our plan was to submit our recommendations to the full IISAC within this time frame, but only after each of our members had had an opportunity to discuss the regulations with departmental personnel of their unit of government familiar with the compliance with the legal requirements contained in the law.

We were informed that we would not be given the 90 days minimum required, but that the regulations were to be in final form by the 1st of December. Therefore our original plans were discontinued a few weeks ago, and our committee has attempted to provide you with our verbal comments and suggestions prior to December 1st. You, of course, have attended all of our committee meetings and have received our comments. I am enclosing for your perusal the comments given to me by a member of the Mayor's staff, Dana Young, as well as a copy of the comments provided by Anne Collopy of the Hennepin County Department of Management Services, all of which I hope will be useful. Other members of IISAC may submit additional comments to me, and I will forward these to you as soon as they arrive.

If you desire, our committee will continue to provide advice to you on draft regulations, but I know that you understand that it is impossible for IISAC to provide you with the type of comprehensive review we would both like to have within the short time span provided.

Very truly yours,

JEROME J. SEGAL
Chairman, Records Management Committee
IISAC

cc: Thomas Anding, Chairman
IISAC

STATE OF MINNESOTA

DEPARTMENT OF ADMINIS ATION

Offic Memorandum

TO : Daniel B. Magraw
Assistant Commissioner

DATE: April 3, 1979

DG

FROM : Don Gemberling
Data Privacy

PHONE: 6-6733

SUBJECT: Data Privacy Rules

I have now completed my review of the Hearing Examiner's Report on the proposed data privacy rules. The Administrative Procedures Act dictates that we evaluate the Examiner's recommendations, accept or reject any changes proposed, make changes to the rules, and submit the revised rules to the Chief Hearing Examiner. The Chief Hearing Examiner then makes a determination of whether there is substantial change between the rules originally proposed and the revised version. If there is not, the Chief Hearing Examiner approves them and returns them to us. To comply with the APA, we must then submit the rules to the Attorney General's Office for their review as to "form and legality."

In the attached report, I have summarized the substantial recommendations made by the Hearing Examiner. I have also made my recommendation as to whether we should or should not follow his recommendations. If a change he recommended was technical and without policy implications, I have not included it in the attached. In case you or anyone else should want to read the full text of the Examiner's findings, I have referred to his recommendations by the finding number in his report.

There are some other factors that you and the Commissioner should be aware of as you consider whether to move these rules forward in the process. First, the media continues to actively oppose certain of the rules, particularly the rules concerning investigative data and arrest information. They either have or will shortly deliver a letter to the Commissioner expressing their opposition. This is necessitated because the Hearing Examiner basically upheld our position on those rules. In my discussions with them, they have indicated they will continue that opposition with the Attorney General if the rules are not changed.

They are also considering legal action, in the form of asking a District Court to enjoin publication of the rules when we file them with the Secretary of State. If we make the changes that the media wants, we will then provoke serious opposition from the other side, particularly from the law enforcement community. Also, I have serious doubts that we can promulgate a rule that will satisfy the media and still get through the Attorney General's review.

Last week, I discussed the status of the rules with Duke Addicks, legislative counsel for the League of Cities. He indicated that the League intends to force the rules into the Legislative Commission for Review of Agency Rules. He was not clear about the timing of that tactic.

Lastly, there are legislative developments that may have a decided effect on the rules as proposed. These developments have not sufficiently crystallized so that I can accurately gauge their true effect. However, Representative Stoa's bill would, if enacted, wipe out virtually all of the statutory language on which the rules are based. Senator Tennessen's bill, which has not yet been introduced, would if passed necessitate some changes to the rules. In my discussions with both of those legislators, I am attempting to minimize the effects of revised legislation on the rules. I am not communicating this as a "cast in concrete" position of the Department. I am only pointing out those places where for stability purposes the language of the current statute does not necessarily have to be changed in light of the rules.

I would appreciate knowing as soon as possible whether I should begin revising the rules based on the Hearing Examiner's recommendations. What the Department intends to do with the proposed rules is also of interest to a number of parties both within and outside the Legislature. We may be asked our intentions in the very near future, particularly in connection with the hearings on Senator McCutcheon's bill concerning investigative data. Those hearings will begin on April 5.

If you have any questions or comments, please contact me. I am providing you with three copies of this memo for distribution to the Commissioner and the Deputy Commissioner.

DG:ln

cc: Sheila Fishman

HEARING EXAMINER'S RECOMMENDATION	MY RECOMMENDATION:
1. We clarify in Rule 1.201 B, concerning scope and purpose, the status of non-proprietary nursing homes. What needs to be clarified is whether such nursing homes, providing residential services to medical assistance recipients, are subject to the privacy act. (Hearing Examiner's finding number 9.) (Hereinafter, the Examiner's findings will be cited as F.N. #)	1. This rule be clarified to bring such nursing homes within the coverage of the act. We review this change with DPW for their input.
2. We clarify in Rule 1.201 D, concerning scope and purpose, that the rules are not intended to affect discovery rules developed pursuant to any statute. (This would include the Office of Hearing Examiner's Rules.) (F.N. 11)	2. The rule as proposed only deals with the discovery issue in the Rules of Civil and Criminal Procedure as promulgated by the Supreme Court. The recommended change would broaden the rule and I agree it should be made.
3. We add to Rule 1.201 D a provision to assure that judges are notified that they are issuing a discovery order covering data that is classified as private or confidential by statute or federal law. (F.N. 11)	3. This suggested change is drawn from a federal rule that attempts to deal with a similar problem. Although I believe we should make this change, it should be discussed with Sheila Fishman before we do so.
4. We make certain minor changes to some of the definitions in Rule 1.202. Those changes were suggested by the St. Paul Mayor's office. (F.N. 16)	4. These are minor items from the policy standpoint. Some should be changed while others should not be changed.
5. Eliminate confusion arising from the "code number provision" of Rule 1.202 C.4. dealing with the definition of data on individuals (F.N. 16)	5. I am not sure this provision is as confusing as the Examiner's report maintains. We should not change the section until we have determined if there is any less confusing way to handle the problem.

HEARING EXAMINER'S RECOMMENDATION	MY RECOMMENDATIONS:
6. Make changes to the definitions of confidential and private data in Rule 1.202 to deal with data that is private or confidential at the discretion of the holder of the data. Specific language suggested by the Hospital Association was recommended by the H.E. The change to the definitions would necessitate changing the rules dealing with access to private or confidential data.	6. We make the changes suggested by the Examiner.
7. Clarify the use of the word "necessary" in 1.202 F., the definition of public data on individuals. (F.N. 21)	7. We clarify the term.
8. Define public data on individuals in Rule 1.202 F., as any data on individuals that is not private or confidential. (F.N. 21)	8. In the proposed definitions, I tried to narrow the "gap theory" as much as possible without killing it. The Examiner's recommendation would effectively kill the theory. His recommendation is based on his assertion that those agencies ultimately bound by this rule will be able to better understand the rule if it is changed. I agree with his recommendation, but with reservations. There is also the strong possibility that the Medical Association (Catholic Bulletin) case has already "killed" the gap theory.
9. Add "unless otherwise provided by state law" language to the definition of responsible authority in Rule 1.202 L. (F.N. 24)	9. I agree.

HEARING EXAMINER'S RECOMMENDATION	MY RECOMMENDATION:
10. Delete Rule 1.203, Access to Public Data. The H.E. found that we do not have the statutory authority to promulgate a rule governing access to public data. Using language from the Medical Association case, his opinion was that such access is governed only by the provisions of Minnesota Statutes §15.17 (F.N. 26)	10. The Department's authority to promulgate rules governing access to public data has always been an open question in our minds. One reason we proposed the rule was to get a reading from an independent legal authority on that question. I agree with the Hearing Examiner's recommendation. Deletion of this rule will necessitate moving a portion of the rule, which deals with computing the cost of providing copies of data to requestors, to another section.
11. Eliminate the requirement, in Rule 1.204 B, of a notarized signature when an individual requests access to private data or dissemination of private data to third parties. (F.N. 31)	11. In his recommendation, the H.E. gave us the out of proposing the notarization requirement as a "may". I recommend we change the rules to include it as a may.
12. We clarify two issues associated with Rule 1.205, Access to Private Date Concerning Minor Data Subjects. Those issues are: 1) Precluding parental access when the minor has not requested such preclusion because of his age or lack of knowledge concerning the parents' request for access. 2) Dealing with individuals who are incompetent to make the request to deny access to their parents. (F.N. 35)	12. We attempt to clarify these two points by making changes to the rules. I use the word attempt because these are difficult issues to deal with in the drafting process. The Legislature has attempted to do so on three occasions and could not come up with generally accepted wording.
13. We further clarify Rule 1.205 access to private data in light of other statutes, particularly M.S. 144.335, which affect the general rule. (F.N. 37)	13. As part of his recommendation, the Hearing Examiner suggested specific language. I suggest we adopt this language.

HEARING EXAMINER'S RECOMMENDATION	MY RECOMMENDATION:
14. Recommends that we provide for an authorized representative of an individual to discover that confidential data about an individual is being maintained in Rule 1.206, concerning access to confidential data. (F.N. 39)	14. I agree with the suggested modification.
15. Amend Rule 1.207, the rule dealing with arrest information, to provide for the release of some information concerning the detention of juveniles. (F.N. 44)	15. We modify this rule by making a reference to release of summary data concerning juvenile arrest or detention.
16. We add a number of agencies to the list of investigative agencies proposed as part of Rule 1.208, Access to Investigative Data. (F.N. 47 & 49)	16. The entire rule dealing with investigative data is controversial. The H.E. recommendation would fan the flames of the controversy without substantially clarifying the issues. I recommend we reject his recommendation. Agencies who expressed concern about certain types of data should direct that concern to the legislature.
17. We add language to Rule 1.209, Access to Summary Data, to either enpower agencies to deny access to private or confidential data or to limit such access to bonafide researchers. (F.N. 51)	17. I do not believe the statute gives us the authority to provide such discretion to agencies by rule. I have discussed this problem with Senator Tennessen and language has been provided in his bill to deal with this issue. To limit access to "researchers" requires definition of that term. Proposing such a definition will raise a whole series of new issues. I recommend we do not make the change recommended by the H.E.

HEARING EXAMINER'S RECOMMENDATION	MY RECOMMENDATION:
18. We delete the requirement that agencies classify public data in Rule 1.210, Classification of Data. (F.N. 54)	18. Changing the rule as suggested by the H.E. would result in a rule requiring agencies only to classify all private and confidential data. By doing so, we would support the theory that all remaining data is public. For clarity purposes, I recommend we make the change suggested.
. We consider putting a lead-time of 12 to 18 months in all rules requiring extensive administrative activity on the part of agencies. (F.N. 55)	19. This was requested by agencies, particularly cities, at the Hearing. Their argument was that they would need this time to request the funding necessary to carry out the activities. Because I can see good arguments on both sides, I have no recommendation.
20. We clarify the reporting requirement in Rule 1.214 to reflect the statutory requirement that agencies need only report on categories of records, files and processes, as opposed to individual files, etc. (F.N. 57)	20. We make the change recommended.
21. We change Rule 1.215, relating to the administration of private and confidential data, to reflect the change proposed to Rule 1.214. (F.N. 59)	21. We make the change recommended. This rule arises from one of the most confusing portions of the statute. Tennessen's bill would clarify this portion of the statute and make it less confusing.
22. We change Rule 1.216, relating to the administration of all data to reflect the change proposed to Rule 1.214 (F.N. 63)	22. We make the change recommended.

HEARING EXAMINER'S RECOMMENDATION	MY RECOMMENDATION:
23. We change rule 1.217, relating to computerized data, so that if an audit of security measures has been conducted within the last year that an audit within 180 days of the promulgation of the rules would not be required. (F.N. 66)	23. We make the change recommended.
24. We change rule 1.217 to require security auditing of all computerized files, not just files that are accessible by terminals. This change was recommended by ISD in a post-hearing comment. (F.N. 67)	24. Make the change as recommended.
25. We change rule 1.218, which deals with administrative appeals of agency decisions to the Commissioner of Administration, to provide for dismissal or rejection of sham or frivolous appeals. (F.N. 68) Specifically, the H.E. suggested language to give the hearing examiner, who convenes the contested case proceeding, the authority to so dismiss or reject.	25. At the hearing, I indicated we would be willing to change this rule by providing for the Commissioner to reject or dismiss sham or frivolous appeals. This change was requested by a number of people because the rule gives this Department the authority to assess the costs of an appeal back to the agency that produced the appeal. For that reason, I suggest we make the change recommended but assign the initial dismissal or rejection authority to the Commissioner. If a sham or frivolous appeal could only be rejected by the Hearing Examiner there would still be costs to agencies generated by the hearing examiner's preliminary review of the appeal.

STATE OF MINNESOTA

DEPARTMENT OF ADMINISTRATION

IN THE MATTER OF THE PROPOSED ADOPTION OF RULES OF THE DATA PRIVACY UNIT GOVERNING THE ENFORCEMENT AND ADMINISTRATION OF THE "MINNESOTA DATA PRIVACY ACT"

STATEMENT OF NEED AND REASONABLENESS

Introduction

Pursuant to Minnesota Statutes 1976, Section 15.1671, as amended, the Commissioner of Administration is required to promulgate rules that will "implement and enforce" the provisions of the Data Privacy Act, Minnesota Statutes Section 15.162 through 15.1671, hereinafter referred to as the Act.

The Act, which was originally enacted into law by the 1974 session of the Legislature has been amended every legislative session since then. These amendments have been the product of a number of factors. These factors include: great public attention to and debate over governmental data handling practices; emphasis placed on resolving data privacy problems by members of the legislature; and research into and public reporting of the effects of privacy legislation by the Department of Administration. (See the Department of Administration's reports to the Legislature concerning the "data privacy act", dated January 6, 1975 and January 12, 1976. Copies of these reports are on file in the Legislative Reference Library.)

Since the effective date of the original Act on August 1, 1974, the Department of Administration has acted as a public resource in the "data privacy" area. This resource activity includes answering questions concerning the Act from both governmental agencies and private citizens. The proposed rules reflect this experience. The need for certain rules, especially in particular areas where the greatest number of questions arose, was clear.

The following describes the need for and reasonableness of each rule or section thereof that is being proposed:

2 MCAR § 1.201. SCOPE AND PURPOSE

Section A: The limits to the application of the Act should be

viewed from two perspectives. The first perspective is concerned with identifying what agencies are subject to the Act. There has been considerable questioning as to whether the Act applies to the private sector's data collection and use practices. Although it is possible to be lead into the false apprehension that the Act does apply to private sector, a careful reading of the Act makes it clear that its application is limited only to governmental agencies of the State. Section A. of this rule makes it clear that the application of the Act is limited to those governmental agencies described in the definitional section of the Act, Section 15.162.

Section B:

There is one exception to the Act solely being applied to agencies that are totally governmental in character. Section 15.162, Subdivision 5 of the Act, the definition of political subdivision, extends application of the Act to "non-profit social service agencies." The language of this extension has created several problems. Section B. of this rule addresses those problems.

The first problem presented is the failure of the Act to define "non-profit social service agency." Section B. provides a workable definition. Without such a definition, it could be argued that all companies and agencies who do any contract work with government are subject to the provisions of the Act. The Act, by additional wording found in Section 15.162, Subdivision 5, is further limited in its application to social service agencies that do their work on account of a contract with a governmental agency. There is an additional need to explain this difficult "contract" language. Parts 1, 2, and 3 of Section B. address the problems discussed above. They are intended to clarify what the language, starting with "to the extent" and running to the end of Subdivision 5, actually means in the context of administrative reality.

The definitions and limits proposed by Section B. emanate from the problems described above. The rule section is necessary so that "non-profit" agencies who do contract with the government can understand what parts of their operation are subject to the provisions of the Act and what parts are not. As an example, one major social service agency carries on over 1500 distinct programs, only twenty of which arise out of contracts with government.

An additional question produced from the application of the Act to only a part of non-profit agency activity is the question of what is the effect of the Act on personnel data maintained by such agencies. It is necessary to draw a line to deal with the personnel question. Subsection 3 of Section B. deals with that question.

The line drawn by the rules would exempt personnel data. This exemption is reasonable in that the method used to bring social service agencies under the coverage of the Act is to connect the agencies to government through the contract mechanism. As the personnel activities of social service agencies would, in most instances, have little or nothing to do with such contracts, drawing a line to exempt personnel records is a reasonable approach.

Section C: The second perspective from which to view the application of the Act is from the perspective of the data in question. For purposes of the Act, governmental agencies maintain two types of data. They are data on individuals and data not on individuals. There have been numerous attempts to apply the workings of the Act, particularly the classification system, to data not on individuals. There is clearly a necessity for the rules to address this question.

Section C. of this Rule makes it clear that the Act is only applied to data on individuals maintained by the governmental agencies. Without such a rule, there would be continuing attempts to apply the Act, which is geared to data on individuals, to data not on individuals. Such attempts will only add to confusion and to the difficulties associated with correctly administering the Act.

Section D. There have been recurring questions concerning the relationship of the Act with other bodies of law, particularly the Rules of Civil and Criminal Procedure. Some individuals have questioned whether the passage of the Act in some ways affects those rules. Because of such problems and questions, it is necessary to clarify the relationship between the Act and the rules. This section of the rule makes it clear that the Act was not intended to affect the operation of either the Civil or Criminal rules.

This problem can be particularly acute when a discovery question arises under either of the rules. Therefore, Section D. is particularly directed to the discovery question. To maintain that the classification system used by the Act can be used to thwart the discovery rights under the court rules requires an attenuated interpretation of the Act. By contrast, the discovery rules are clear and are a fundamentally important provision essential to the workings of the judicial system. Comparing the interests represented by the discovery right under the rules with an attenuated interpretation of the Act used to thwart that right makes it clear that the latter interpretation cannot stand. Section D. is necessary to clarify which interest should be preeminent. There is at

least one Minnesota District court case that supports the position taken by the rule on this question. (See decision of Judge P. Fitzgerald, in Smith v. County of Hennepin, Fourth Judicial District, File Number 739819, May 5, 1978.)

Section E. Another question that occurs with some frequency is concerned with the relationship of the Act to various judicial orders, including such things as orders to produce data or orders to seal data. There have been questions regarding whether such orders produce conflicts with the Act. It is necessary for the rules to clarify, for those charged with administering the Act, which authority should be preeminent in a given situation. The rule makes it clear that judicial orders will enjoy preeminence when any supposed conflict occurs. This is another point at which some line must be drawn. The consequence of not drawing such a line may make it impossible for either the Act or the judicial system to operate. Because such judicial orders will arise from an understanding of all of the facts and circumstances of a given case, and not from the very generalized non-specific operation of the Act, it is more reasonable to give judicial orders preeminence.

Section F. Section 15.1671 clearly states that no rules can be written that will affect the provisions of Section 15.165, the Rights of Subjects of Data. However, within the Act, there is a semantic and logical connection between Section 15.165 and other provisions of the Act on which rules can and should be written. However, the requirement of 15.1671 must be met. Therefore, Section F. is presented to assure that while a given rule may touch on some point connected to, or even a part of, Section 15.165, such a rule is not intended to and shall not diminish the rights that are expressed in Section 15.165.

Section G. This section of the rules is necessary to emphasize the overall interests that are balanced by the Act, the rules and also by those charged with administering the Act in an operational context. It is reasonable to provide such a statement of the interests to be balanced because recognition and awareness of the interest balancing can be helpful to making the day-to-day decisions concerning the administration of the Act. This emphasis on balancing competing interests follows the approach taken by the Minnesota Legislature in its evolution of privacy legislation since 1973.

2 MCAR § 1.202. DEFINITIONS The definitions contained in this section are of two types. Some terms which are not found in the Act are defined because they are necessary to the operation of the rules. The second type of definition deals with terms that are found in the Act, but which require further clarification by the rules.

A statement of the necessity for and reasonableness of each definition follows:

A. ACT: This definition is necessary for the purposes of the rules. The term is defined so that the "shorthand" term Act can be used throughout the body of the rules without having to resort to the complete legal citation of the various statutory sections.

B. ARREST INFORMATION: This term was first placed in the Act in 1976 to deal with a problem that arose out of disagreements between representatives of the news media and law enforcement officers after the 1975 amendments were made to the Act. (See "Police Interpretation of Privacy Law Brings Changes of Withholding Data", Jack Coffman, Minneapolis Tribune, January 11, 1976. and "Panel to Attempt Privacy Law Changes", David Kuhn, Minneapolis Tribune, January 13, 1976. Copies of these articles are attached and labeled Attachment #1.) The term has a specialized meaning within the operation of the Act. Unfortunately, for classification purposes, the language of the Act uses a technique of defining what "arrest information" is not. This rule is necessary to establish the specialized meaning of the term and also to define what "arrest information" is.

There are a number of governmental entities that collect something that could be called arrest data. Such data is often collected on employment application forms. It is not clear on the face of the Act whether it was intended for the term "arrest information" to extend to employment related arrest data. The rule makes it clear, given the legislative context that produced the "arrest information" definition in the Act, that such information is limited to that collected by law enforcement agencies.

The reasons for which this particular language was added to the Act makes it reasonable to limit arrest information in such a way. Generally, those reasons can be summarized in the statements, expounded by a legislative author in open hearings, that there should be "no secret arrests" made in this state by law enforcement agencies. (See "Privacy and the Right to Know", State Senator Robert J. Tennessen, Minneapolis Star, February 16, 1976, a copy of which is attached and labeled Attachment # 2.

C. DATA: This definition has two purposes. First, it is a way of introducing a shorthand method of referring to the term actually used by the Act, which is "data on individuals." Second, there has been considerable confusion and numerous questions as to how all-encompassing is the definition of data on individuals. Much of this confusion stems from the fact that the Act's definition uses the terminology "is or can be identified." Sections 1 through 5 of this section deal with the most common situations and questions that have been raised as to the extent of the coverage of the defined term. It is necessary to define this term as clearly as possible. Without such clarity, administrators would not be able to deal with the basic subject matter of the Act, which is data on individuals and how to administer it. Because of the language of the Act's definition, it would not be reasonable to deal with this definition in any fashion other than that adopted by the rule. It is clear from the "is or can be identified" language of the Act, that it was intended that this definition should be all-encompassing.

D. CONFIDENTIAL DATA: This term, as defined in the Act, is actually stated in terms of who can gain, and who is denied access to a certain type of data. Because of that form of the statement, it is necessary to make more clear how it is determined that certain data is confidential, as opposed to private or public. Determining the proper classification of all agency data is absolutely necessary to proper administration of the Act. That determination depends for its first step on a correct reading of the definitions of the three classifications. This definition is intended to assist governmental personnel in determining, according to the requirements of the Act, what data is confidential in their agency.

The term "confidential" has the specialized meaning given to it by the Act. That meaning is not the same as the common generic everyday usage of the term confidential. The rule is intended to clarify what the term confidential means in the context of the Act. To assist in that clarification process, Sections 1 and 2 of this definition provide some common usages of the term confidential. The rule then points out whether or not the usage gives to the term confidential the usage that is intended by the Act.

E. PRIVATE DATA: The term private was incorporated into the Act in 1975, thereby providing a means of differentiating between data that is not available to the public or to the data subject (confidential data), and data that is not available to the general public but is available to the data subject (private data). The private term has the same basic limits placed on it by the Act, in terms of how something becomes private, as does confidential. The classification of certain data as private requires that there be clear legal authority for that classification. The term private is also stated in terms of who can gain and who is denied access to data that is actually private.

Because the term private, as an access term, is unique to Minnesota, it is vital for the administration of the Act that personnel administering the Act be provided with the greatest possible clarity. The rule fulfills this need by making it very clear what requirements must be met before certain data can be determined to be private data. As with confidential data, the rule uses the technique of presenting common ways that the term might be used in the context of legal authority and whether that particular usage means that data <u>is</u> or <u>is not</u> private for the purposes of the Act.

This rule also deals with the problem of statutes that were passed prior to the initiation of privacy legislation in 1974. In some instances, those statutes, which use the term confidential, are intended to deny access to the public but to extend access to the data subject. In most instances, the term confidential is used,

followed by language that modifies the term. It is vital for personnel administering the Act to be made aware that when the legal authority they are using to classify uses that kind of approach, that the data in question should properly be classified as private and not confidential. The generic term confidential does not control in such situations. A full reading of the appropriate authority is what controls. The rule provides clarity on this confusing point.

F. "PUBLIC DATA ON INDIVIDUALS". There has been and continues to be considerable confusion and controversy surrounding this particular definition. An understanding of this term is necessary so that personnel administering the Act will be able to administer the three part classification system. Continued confusion concerning this term is a major obstacle to successful implementation and administration of the Act. For those reasons it is vital that the definition of this term be as clear as possible.

The confusion primarily stems from the fact that the Act attempts to define public data by incorporating, by reference, the definition of public record from Minnesota Statutes, Section 15.17. Unfortunately, nowhere in Section 15.17 is the term public record clearly defined. The rule attempts to provide a clear definition by adopting the definition postulated by the Minnesota Supreme Court in the case of Kottschade v. Lundberg, 280 Minn. 501, 160 N.W. 2d 135 (1968). In addition, the rule expands on the Court's definition by further defining various types of data that should be public because they bear a close relationship to official acts taken and functions carried on by governmental agencies. As with the adoption of the Court's definition, the necessity for the expansion is found in the vital need for clarity of direction to governmental personnel as they administer the three-part classification system.

The definition, as proposed by the rule, is reasonable in three respects. First, the definition tries to parallel the view of the data held by those who maintain the data. If governmental personnel feel that certain data is necessary to their operation of governmental agencies and programs, it seems clear that access to that information is equally necessary to anyone trying to understand a particular governmental agency or program. Second, failure to set forth a clear definition of public data makes the question of what is public a subject of continuous litigation. Without a clear definition, agencies are forced to adopt a cautious approach which results in denial of access by the public. This denial then results in litigation by the public. This cautious approach is dictated by the varying remedies provided by the Act and implicit in Minnesota Statutes § 15.17. The remedy for denial of access to a record declared public is production of the record. The remedy for improper disclosure of private or confidential data may be money damages or even criminal penalties under Sections 15.166 and 15.167 of the Act. Third, continued confusion in this area leaves agencies open to potential liability. Without a workable and realistic definition of public data, agencies will continue to

be unable to properly implement the Act. Failure to implement presents possible liability under the penalty provisions of the Act.

G. DESIGNEE: The Act provides the responsible authority with the authority to appoint individuals to assist him or her in the administration and implementation of the Act. Designee is merely the shorthand term adopted by the rules to provide a title for individuals so appointed.

H. ENTITY: This definition is necessary to provide both a shorthand term to refer to agencies of government that are subject to the Act, and to provide more clarification than that offered by the Act as to the agencies that are regulated by the Act. In referring to regulated agencies, the Act uses the terms state agency, political subdivision, and state-wide system. Although the first two terms have a generally accepted meaning, that meaning is subject to misunderstanding. This definition is necessary to eliminate any confusion and misunderstanding, and to assure that each agency of the state is aware of the fact that it is either subject to, or not subject to the Act. Although the term state-wide system is defined by the Act, a clearer statement of the definition is necessary to assure that all state-wide systems are indeed regulated.

I. FEDERAL LAW: Although this term is used at several critical points in the Act, and a clear understanding of the term is necessary for implementation of the Act, it is not defined by the Act. A further complication is that there appears to be no generally accepted legal meaning of that term. This rule is necessary to provide a clear and guiding definition. The definition as proposed would include all possible types of legal pronouncements emanating from federal law.

The overwhelming majority of personnel charged with the administration of the Act are laypersons, not attorneys. A simple and easy to understand definition of the concept of federal law, as it relates to the workings of the Act, is necessary for reference by such persons.

J. INDIVIDUAL: This term is defined in the Act. However, there are persistent questions concerning the Act's application in two areas relating to the definition of "individual." The first question can be summarized as: Are records maintained on persons who are no longer living subject to the Act? The proposed definition fills the need of answering that question. The proposed rule gives a negative answer. Such an answer stems from a widely accepted legal principle, stemming from both the defamation and privacy torts. In defamation, this principle generally holds that relatives of dead persons have no rights to recover for damages to the reputation of the deceased. (See Corpus Juris Secundum, Volume 53, "Libel and Slander" § 145, p. 230.) In privacy, the principle is one that it is conceptually impossible to invade the zone of privacy of one who is not living. (See Corpus Juris Secundum, Volume 77, "Right of Privacy", § 1 c., p. 398. See also, Smith v. County of Hennepin, supra.)

The second question often asked about the Act as it relates to the definition of individual is: Does the Act apply to records concerning business, a business entity when the name of that entity is the same as a natural person? The rule proposes a negative answer to this question. The rule definition is drawn from the terminology used in the Act. The Act uses the term "natural" which modifies individual in Subdivision 4 of Section 15.165 "individual". In legal usage, the term individual, particularly when it is modified by "natural" refers only to living human beings, not to entities which are licensed into existence by the State. (See the definition of "person" in Black's Law Dictionary, Henry C. Black, Revised Fourth Edition, West Publishing Co., 1968, p. 1299.) However, this legal usage is not generally known to laypersons. Therefore, clarification on this point is necessary to proper administration of the Act.

K. RECORDS MANAGEMENT ACT: This is a shorthand term used to refer to a section of Minnesota Statutes that bears a close relationship to the Act. The use of a descriptive title for this Act, instead of the legal citation, calls attention to the fact that there is a statute that bears directly on the question of proper disposition of records.

L. RESPONSIBLE AUTHORITY: No actor in the administration of the Act is more important than the responsible authority. Although the Act clearly requires that there be one individual carrying on the responsible authority function in each agency covered by the Act, the Act's definition of the term is not clear. The Act's definition has produced a number of questions. The most common of those questions are: 1) Can there be multiple responsible authorities in a single agency? 2) When the agency in question is a state agency which has no commissioner, who should the responsible authority be? 3) In reference to state agencies, what does the phrase "designated by law or by the Commissioner" mean in the first sentence of Subdivision 6 of Section 15.162? 4) In reference to political subdivisions, what does the phrase "unless otherwise provided by law" mean in the last sentence of Subdivision 6 of Section 15.162? Because of the pivotal role played by the responsible authority in the Act, this definition is necessary to state exactly who the responsible authority ought to be in each governmental agency. This definition, plus rule 2 MCAR § 1.212 should answer virtually all current questions asked about the identity and appointment of the responsible authority.

M. SUMMARY DATA: Although this term is defined in the Act, personnel charged with the administration of the Act have raised many questions concerning the definition. Among those questions are: 1) Can summary data be extracted from public data? 2) Is summary data the same thing as statistical data, or is it something more? 3) What kinds of things are summary data?

The concept of summary data plays a very important role in the Act. It presents a method by which individuals and other persons

can, for research and other purposes, have access to private and confidential data concerning subjects of government data. Because of the summary data concept, this can be done without revealing the identities of the subject of data. The summary data concept is particularly important to the interests of researchers, academicians and the news media. Without a clear understanding of the term "summary data", those interests will not be served and individuals charged with the administration of the Act will not be able to correctly administer the Act. The expanded definition of summary data which is proposed by the rule, particularly the examples of what is summary data set out in points 1. and 2. of the definition, coupled with 2 MCAR § 1.209. Access to Summary D Data, are intended to provide the information and guidance necessary for such personnel to properly administer the Act.

INTRODUCTION TO RULES 2 MCAR § 1.203, 204, 205, 206, 207, 208, and 209:

There is no concept contained in the Act that has generated more questions and confusion than the general subject of access to various types of data. It is very common for governmental agencies to maintain that certain data cannot be accessed by the public or by an individual data subject "because of the privacy law." Such a statement is an absolute misnomer when it is used in reference to the Act's handling of private and confidential data. With limited exceptions the Act itself does not classify any data as private or confidential. The Act does prescribe certain uniform treatment concerning access to data classified as private or confidential only when other law, state statutory or federal, determines the actual data classification.

The exceptions referred to by the previous paragraph deal with certain types of data for which the Act does prescribe a classification or a certain access treatment. Those types of data are: private data concerning data subjects who are minors, active investigation data, summary data, and arrest information.

The general thrust of the rules enumerated above is to deal in a uniform fashion with the most common questions raised about access to each type of data covered by the provisions of the Act. There are a number of common problems with dealing with access as it relates to each type of data. These problems are dealt with in the proposed rules by adoption of parallel treatment in the early sections of each rule. Following that parallel treatment, each rule deals with the unique problems or questions presented by the Act's handling of a certain type of data.

The necessity for each of these rules stems from the Act's implicit requirement that data of the same type receive uniform treatment throughout the state. This need for uniformity also stems from an understanding of the current experience with the Act. Individual citizens should not have to learn and to follow an entirely different set of access procedures each time they go

to a different governmental agency and make a request to gain access to data.

While acknowledging the necessity for the general uniformity of treatment of access to data, the aforementioned rules also acknowledge that in certain areas, the methods of disseminating data may vary from agency to agency. This variance in exact treatment will be reflective of internal factors present in the agency. These factors will include size of the agency, number of records maintained by the agency, and numbers and types of personnel assigned to administer the requirements of the Act. Obviously, access to data will not be treated, in the particulars of public administration, in the same fashion in Funkley, Minnesota as it is in Hennepin County. The rule acknowledges thas agency variance by delegating the preparation of the exact procedures determining access, within the requirement of the rules, to the Responsible Authority in each agency.

A discussion of specialized problems associated with each of the rules dealing with access follows.

2 MCAR § 1.203. ACCESS TO PUBLIC DATA

Section A: This rule is needed to describe exactly, in general terms, who is given access to public data. The rule attempts to deal with the modern principles of access to government records by rejecting the common law rule that the person seeking access to public records needs to demonstrate an interest in that particular record.

Because of the multiplicity of governmental functions and the varying ways of maintaining public records, the rule directs the responsible authority to establish the detailed procedures necessary to provide access to the public data of his agency.

In Section A, Subsection 1.c., the rule acknowledges that there are costs incurred in providing public access that should be recovered by the governmental agency. The public data definition of the Act incorporates the provisions of Minnesota Statutes, Section 15.17 by reference. Subdivision 4 of Section 15.17 has some language dealing with payment of fees for receipt of copies of public records. However, that language is not clear because Subdivision 4 uses the phrase, fees "prescribed by law." In many agencies, this phrase has no meaning. Subsection d. of this section, which deals with recovery of agency costs, is intended to fulfill the need of informing agencies of the cost factors that can be used in determing what the public should be charged for receipt of copies of public data.

By providing for recovery of costs, the rule is a reasonable attempt to require that those who receive some type of benefit from access to and use of public records should be those who bear the costs of providing those records. The mass of taxpayers do not make large scale utilization of public records. If agencies

merely bore the costs of providing copies without charging the cost back to the actual users of public records, taxpayers of the state would be paying, through increased taxes, for benefits enjoyed by a very few.

2 MCAR § 1.204. ACCESS TO PRIVATE DATA

Section A: This rule is needed to describe exactly who is given access to private data. By specifying types of individuals and agencies given access to private data, the rule answers many of the most commonly asked questions concerning access to private data. In particular, the rule in Subsection 4 makes it clear that any individual, who is the subject of private data, can direct the government agency holding that data to make it available to other persons. This part of the rule reinforces an underlying rationale of the Act which is that data subjects retain some control over the data they provide to the government.

Section B: Because of the variations in the ways that private data may be retained, the rule directs the responsible authority to develop the detailed procedures to provide access that he or she feels are necessary in his/her particular government function. The Act places a high value on the right of individuals to gain access to governmental data maintained about them. To assist them in gaining that access, the rule requires that the procedures be in writing so that individual data subjects are provided with information as to how exactly they may gain access to data recorded about them.

Subsections 1 and 2 of this section deal with a logical problem presented by the language of the Act. The problem presented is not covered by the Act itself. It is necessary to the proper administration of the Act to assure that any person who requests access to private data is actually the subject of that data. Subsection 2 fills the need of prescribing guidance to the responsible authority for the handling of this problem in agency procedures.

Section C: This section deals with another problem presented by, but not dealt with by the language of the Act. This is a timing question concerning when a subject may gain access to data concerning himself or herself. The section fills the need of prescribing the time when access may be gained. Normal working hours is the most reasonable time to make, and to be able to expect, to gain access to governmental records.

Sections D and E: The question of whether a data subject may be charged a fee for viewing and copying data concerning that subject is a recurring one. The Act, while providing for free access by the data subject to that subject's data, requires the responsible authority to charge data subjects for any copies of private data

they receive. This seeming anomaly makes it necessary for the rule to provide guidance in two areas. First, the rule makes it clear that when the data subject only desires to view private data concerning himself or herself, there shall be no charge made either for the opportunity to do that viewing or for the viewing itself. Second, the Act's requirement that the responsibile authority charge for providing copies of private data must be subject to some reasonable limits. The rule proposes charging limits for receipt of copies of private data to be the same as those provided for public data. If no reasonable limits were placed on the assessment of costs for providing copies, agencies might, by charging exorbitant fees, be able to effectively deny the individual's right to receive copies.

2 MCAR § 1.205. ACCESS TO PRIVATE DATA CONCERNING DATA SUBJECTS WHO ARE MINORS

The Act provides for dual access concerning private data maintained on individuals who are minors. Several questions have been raised in regard to this requirement. This proposed rule attempts to deal with the most common questions.

Sections A and B: These sections of the rule follow the parallel construction adopted for all of the rule sections dealing with access. These sections make it clear that private data on minor subjects is still private data, which makes such data subject to all of the basic requirements concerning private data which occur throughout the rules.

Section C: Although the Act does provide for parental access to private data concerning that parent's minor data subject, access is subject to a significant exception. The exception is set out in the definition of "Individual" in Subdivision 4 of Section 15.162 of the Act. Proper implementation of the Act requires that the limits represented by this exception be clearly expressed. This exception has produced an abundance of questions, particularly from educators and social service agencies. The proposed section attempts to answer those questions.

The right of parental access is tempered by authority, given to the responsible authority by the Act, to deny such access when it is in "the best interest of the minor" to do so. Although this consideration of best interest is required by the Act, the Act does not provide guidelines by which the responsible authority can test "best interest." To fill this need, the rule provides five individual standards which the responsible authority must use in assessing "best interest." These five were chosen as the most reasonable to bring to the attention of the responsible authority because they appear to be the most critical.

2 MCAR § 1.206. ACCESS TO CONFIDENTIAL DATA

Sections A and B: Generally, these sections of the rule follow the parallel construction adopted for all of the rule sections dealing with access. Section A. fulfills the need of describing exactly who can gain access to confidential data. Section B. fulfills the need of assuring that data access is limited to those persons identified in Section A. by requiring the responsible authority to develop procedures to control access. The section also fulfills the need of providing guidance to the responsible authority concerning detailed requirements that should be made a part of such procedures.

Section B. Subsection 1,a: This section of the rule makes it clear that the responsible authority has the authority to deny access to data that is properly classified as confidential to any subject of such data and to the public. However, the rule also makes it equally clear that any subject of confidential data has an absolute right to know that he or she is the subject of confidential data. The statutory language is somewhat confusing on this point. In Section 15.165, Subdivision 3, the Act refers to individuals being informed if they are the subject of any data. The next sentence then speaks of individuals gaining access to private or public data. The rule is necessary to eliminate the confusion that results from the interplay of those two sentences. This clarity is necessary to assure proper administration of the Act. This particular provision is based on a concept, implicit in the Act, that there shall be no secret files maintained on individuals in this state.

Section B. 1., Subsections b and c: Because of the sensitive nature of confidential data, even the mere fact that an individual is the subject of certain types of confidential data should not be known to the general public. To fulfill this need, while balancing the individual's right to know he is a data subject, these parts of the rule provide certain guidelines to be followed by the responsible authority to assure that only the person who is the actual subject of the data learns that he is such a subject. This part of the rule is necessary to handle a logical problem which is implicit in the requirements of the Act, but which is not the subject of explicit language of the Act.

2 MCAR § 1.207. ACCESS TO ARREST INFORMATION

Because of the wording of the Act, the question of who is given access to arrest information and how long that access is available is subject to considerable confusion. The Act makes it clear, in Subdivisions 2a and 5a of Section 15.162, that arrest information is neither confidential nor private data. It is left to the reader to interpret by a process of exclusion that arrest information must be public. However, the Act also modifies the definition of arrest information in these private and confidential data definition sections, by referring to arrest information as

being reasonable contemporaneous with the arrest or incarceration.

It is clear that the words "reasonably contemporaneous" were intended to place a limit on general public access to the elements of data that comprise arrest information. The term "reasonably contemporaneous" was originally drawn from the federal Department of Justice rules concerning access to criminal history information. (See Subpart B, Rule 20.20 (c) in the proposed rules of the Department of Justice governing Criminal Justice Information Systems printed in Volume 40, number 98 of the Federal Register, May 20, 1975.) It was intended that the state statutory provisions be harmonious with the federal rules. Unfortunately, the phrase "reasonably contemporaneous" was subsequently deleted from the federal rules.

Section A: This section acknowledges and deals with the classification problems by making it clear that arrest information is public, but limiting the public classification only to a duration of time that begins with the actual arrest.

Section B: To explain the term "reasonably contemporaneous", this section proposes and defines a definite period of time during which arrest information must be made available to the public. The classification of arrest information after that period of time is subject to applicable provisions of statute or federal law.

Section C: There are clearly situations in which there is a high level of public interest in a given crime and the individual(s) arrested for that crime. Given the Act's definitions of "arrest information" and the administrative discretion that is implicit in the definition of "investigative data" it is clear that the responsible authority has some discretion to release additional data. However, the responsible authority needs guidance to balance the competing interests that come into play in such situations. This section provides that guidance.

The rule proposes that certain elements of data, concerning the arrested individual and the alleged crime, beyond those listed in the definition of arrest information may, in the public interest, be released. Such data elements would normally be drawn from the type of data referred to as investigative data, which is assigned the confidential classification by the Act. However, while assigning the confidential classification, the Act also makes it clear, subject to the limitations of 15.162, Subdivision 2a, (b), that the responsible authority has discretion to designate certain data as investigatory data. The proposed rule works within that discretionary authority to allow certain data associated with the arrest to be moved from the investigatory type of data into public data.

The rule's provision for this exercise of discretion was deemed necessary and reasonable because of high public interest in and concern with crime events. The responsible authority's exercise of this discretion is subject to certain factors that must be

taken into account before the discretion can be exercised.

Section D: In Section 15.162, Subdivision 1a, the Act determines whether "arrest information" concerning juveniles is public by referencing the statutory section which controls juvenile records, Section 260.161. The Act further excludes data created pursuant to Section 260.161 from the definition of "arrest information." This handling of juvenile "arrest" data has produced a number of questions. This section of the rules fulfills the need of providing answers to those questions. The section also provides the clear guidance to the responsible authority which is necessary to acheive the desired compliance with the requirements of the Act.

2 MCAR § 1.208. ACCESS TO INVESTIGATIVE DATA

The language of the Act, Section 15.162, Subdivision 2a, (b) makes it necessary for the rules to provide guidance to responsible authorities in their exercise of discretion in designating certain data as investigative data. Because investigative data is classified as confidential, it is necessary for the rules to clearly describe and tightly limit the exercise of that discretion. The Act does give the responsible authority certain discretion, subject to three criteria that will be discussed below, to designate certain data as investigative. However, nowhere in the Act is the term investigative data defined. The balance of this rule is devoted to defining that term and to providing limits on the responsible authority's discretion to designate certain data as investigative.

Section A: Because of the sentence structure and the punctuation of the statutory section, it is necessary for the rule to clarify that investigatory data is confidential data. As confidential data, investigative data is subject to the same basic rules concerning use of and access to any confidential data.

Section B: To provide guidance to the responsible authority in determining what investigatory data consists of, this section of the rule sets forth three criteria that must be met before any data can be determined to be investigatory data. The confidential classification, as applied to investigatory data, presents a potentially serious problem. As confidential data, investigatory data can be withheld from both data subjects and the general public. This condition prevents the operation of checks on agency abuse represented by either the subject's demand for correction or the possibility of public exposure through public access. Therefore, it is necessary that this exercise in discretion operate within the tightest possible guidelines. The rule presents those guidelines as criteria that must be met before any data can be designated as investigatory data. The criteria are drawn from the implied definition of investigative data found in 15.162, Subdivision 2a.

The three criteria that must be met are referred to in the rule as: 1) the collecting agency criteria; 2) the purpose of collection criteria; and 3) the active data criteria. Requiring the responsible authority to determine that the data in question can meet all of the criteria is the method adopted by the rule to assure that this exercise in administrative discretion operates within the requirements of the Act, and with the minimum possible abuse of discretion.

Section B: In Section 15.162, Subdivision 2a, (b), the Act refers to data "collected by a civil or criminal investigative agency." The term "civil or criminal investigative agency" is not defined by the Act and there does not seem to be a generally accepted definition for the term. This part of the rule fulfills the need of providing a definition for the quoted term. Without such a definition, it is conceivable that any governmental agency could maintain that it is a "civil or criminal investigative agency" and thereby attempt to withhold certain data from public access. The definition of the term is necessary to provide agencies with guidance so that they can properly determine whether they are or are not such an agency.

Section B. 2: In Section 15.162, Subdivision 2a (b), the Act refers to data collected "for the purpose of the commencement of a legal action." It is obvious that civil and criminal investigative agencies do collect substantial data that is not for the purpose of commencing a "legal action." The term quoted from the Act is present to provide another limit on the types of data that can be moved into the investigative rubric. "Legal action" may, and there appears to be some question about this, have a generally accepted meaning among attorneys. However, the term "legal action" does not seem to have a generally accepted definition among lay persons. This section of the rule is necessary to provide an understandable definition. Without such a definition, investigative data might be expanded to cover types of data that were not intended to be covered by this section of the Act. The section is also necessary to provide guidance to the responsible authorities in their determination of whether certain data is investigatory.

Section B. 3: In Section 15.162, Subdivision 2a (b), the Act refers to data collected "as part of an active investigation." However, the Act does not provide guidance as to what constitutes an "active investigation." The rule is necessary to provide guidance. Without such guidance, an agency could maintain, merely by saying so, that all or a substantial part of its data is "active." This part of the rule is intended to provide the necessary limits on the responsible authority's discretion to label data as "active." The rule must do so because no limits are provided by the Act. Because "active" is only understandable as a reference to time, the rule section provides time references within which certain data are and will continue to be active until a

designated point in time. This is a reasonable approach to the "active" data problem because agencies will be able to specifically place their data within a specific time frame. By doing so, they will then be guided as to whether the data is in fact "active" for the purpose of determining whether it is investigative.

2 MCAR § 1.209. ACCESS TO SUMMARY DATA

In its handling of summary data the Act acknowledges that "privacy" legislation may have a negative impact on the public interest in research concerning the operation of government and its programs. The technique developed in the statute to avoid this negative impact involves the summary data definition and the specific provisions of the Act governing summary data. The rule is written to provide responsible authorities with the guidance they need to properly administer the summary data provisions of the Act.

Section A: Because of the wording of the Act, there has been considerable confusion as to whether summary data must be legally classified as public before it can be accessed by the public. In Section 15.1641 (d), the first sentence refers to the ability to use summary data "provided that summary data is public pursuant to section 15.17." However, the very next sentence mandates that the responsible authority prepare summary data "upon the request of any person." This section of the rule is necessary to eliminate this seeming contradiction.

Section B: The Act presents a flexible approach to the subject of preparation of and access to summary data. The rule establishes certain necessary limits drawn from the Act to guide this flexibility. These limits are designed to handle the detailed requirements that are not established by the Act itself. The rule makes it clear that the Act proposes a process by which summary data can be prepared from private of confidential data. The rule further clarifies that any person can request or can actually summarize data from private or confidential data.

Because there may be costs associated with providing summary data, there is a need to provide the responsible authority with guidance concerning the assessment of such costs. Without such guidance, agencies could actively discourage usage of summary data by making costs prohibitive. Subsection 2 of this section provides the responsible authority with the necessary guidance concerning reimbursement of costs associated with providing summary data.

Although the Act clearly requires the preparation of summary data upon request by any person, the provisions of the Act produce some confusion as to what that preparation requires in the administrative context. The rule attempts to eliminate this confusion by providing definitions and by setting out in Subsection 5 some of the more common methods to be used in preparing summary data.

The rule also uses Subsection 5 of this section to deal with a common problem that has arisen, particularly between representatives of the media and plice agencies. This problem is concerned with providing public access to private or confidential data when the interest represented by such access could be served by providing data that does not identify specific individuals. There is sufficient flexibility in the summary data provisions to categorize certain reports, such as police incident reports with all personal identifiers stripped from them, as summary data. By doing so, the media is provided with sufficient data to to report crime and other incidents to the public. However, by use of the summary data provisions, protection is afforded to the integrity of police investigations and identies of victims, informants, and so forth.

The Act clearly permits a person outside the agency to summarize data from private or confidential data. However, the Act does not provide the responsible authority with detailed guidance to admister that requirement. This section provides those guidelines. To protect the actual private or confidential data being manipulated by a person from outside the agency, the Act provides for a non-disclosure agreement. However, the Act does not specify the contents of such an agreement. Subsection 4 of this section provides the necessary guidance to the responsible authority by setting out minimum contents of such an agreement.

2 MCAR § 1.210. CLASSIFICATION OF DATA

The Act imposes a number of administrative duties and requirements on the responsible authority. The exact nature of the responsible authority. The exact nature of the duties to be performed varies according to the classification of the data maintained and used by the governmental agency. Because of this variance in requirements, the responsible authority must, as a first step toward proper implementation of the Act, determine the proper classification for all data maintained by the particular agency. This rule makes it clear that classification of data is a positive duty that must be performed, by the responsible authority. Without this duty being performed, the Act cannot be properly implemented in the entity.

Sections A through D of this rule set forth the reasonable steps that should be taken to comply with the classification requirement. The steps to be taken are a logical progression beginning with identification of all the data being maintained by the agency. If these steps are not followed, and the appropriate actions taken by the responsible authority, it will be impossible for the agency to comply with the detailed requirements of the Act.

2 MCAR § 1.211. AUTHORITY OF THE RESPONSIBLE AUTHORITY

The necessity for this rule arises from two problems in the Act. First, the duties assigned to the responsible authority by the Act are voluminous. Notwithstanding this long list of duties, there is no explicit statement of the authority of the responsible authority to carry out all the requirements assigned to that position. Authority must be read as being implicit in the many duties. This rule takes that implicit but unstated authority and expressly states that the responsible authority has the authority to do these things required of him/her by the Act.

Second, the one place in the Act where it may be said that there is an express assignment of authority to the responsible authority is in Section 15.1641 (a). Unfortunately, the Act uses the term jurisdiction to describe the authority. Jurisdication is a legal term of art which has little or no meaning to those laypersons who are responsible authorities. Furthermore, jurisdiction in its proper legal usage is a term that has no relevance to purely administrative functions. This rule is intended to make it clear that the term jurisdiction, as used in the Act, is a term conferring authority on the responsible authority. Sections A. through B. of this rule go on to expressly state the limits on and the detail of that authority.

2 MCAR § 1.212. APPOINTMENT OF THE RESPONSIBLE AUTHORITY

Section A: The requirement of the appointment of a responsible authority in certain political subdivisions is the express subject of one provision of the Act, Subdivision 6 of Section 15.162. However, the necessity for such an appointment is not made clear for certain other types of governmental agencies. Practical experience with the implementation of the Act makes it clear

that appointment of responsible authorities has often not been accomplished as required by the Act. This section fulfills the need of clearly directing certain governing bodies to accomplish that appointment.

Section A. 2: Given the lack of clear authority conferred on the responsible authority by the Act, there is a further need for the responsible authority to receive the requisite authority from his or her employer, the appointing governing body. Without such a clear conferral of authority, it may be impossible for the responsible authority to perform the duties assigned by the Act. This rule deals with these two needs by making it clear that a responsible authority must be appointed, and furthermore, that the responsible authority so appointed must be given sufficient administrative authority by the governing body to take the actions necessary to comply with the Act.

Section A. 3: To assist governing bodies in making the formal appointments, forms have been created and placed in the Appendix to these rules. These advisory forms have been drawn from actual forms previously used to appoint responsible authorities in various agencies.

2 MCAR § 1.213. APPOINTMENT POWER OF THE RESPONSIBLE AUTHORITY

In Section 15.164 (a), the Act does provide authority to the responsible authority to appoint individuals to assist in the implementation and administration of the Act. The grant of appointment authority in the Act is simply a grant with no detailed explanation of the form of the appointment or limits placed on the appointment authority. This rule is necessary to provide for formalities of the appointment and to set out limits on the authority.

Section A: Because designees may be the personnel who deal with the public and with data subjects, it is necessary that there be a written record of any appointments. To satisfy this need, the rule requires that the actual appointment of a designee be accomplished in writing.

Section B: The primary purpose of the designee appointment power under the statute is to provide the means for the responsible authority to share the administrative duties associated with the implementation and administration of the Act in the agency. For designees to be able to perform such functions, the responsible authority must provide them with sufficient guidance as to the Act's requirements. To fulfill this need, the rule proposes certain activities that must be carried on by the responsible authority if the appointment authority is exercised. The objective of these activities is to assure that designees will be properly instructed and directed in performing the duties of the responsible authority under the Act.

2 MCAR § 1.214. DUTIES OF THE RESPONSIBLE AUTHORITY AS THEY RELATE TO PUBLIC ACCOUNTABILITY

This section is needed to provide guidance to responsible authorities in complying with the Act's requirement that a document be created that describes certain aspects of the agency's data administration program to the public.

Section A: The Act requires the general public and individual data subjects to direct their requests to access data and to make other inquiries to the responsible authority. In order to comply with this requirement, it is vital that the identity of the responsible authority be made known to the public. This requirement is intended to be satisfied by the public document required by Section 15.163. This section of the rule provides a temporary method by which at least the identity of the responsible authority shall be made available to the public until such time as the complete document required by the Act is prepared. Given the authority of the responsible authority to appoint designees, there is a further need for the identity of such designees to be made available to the public. The rule prescribes the method by which this identification will be accomplished.

Section B: The proposed rule would add certain items to the contents of the public document in addition to those items required by Section 15.163. The need for the additions proposed by the rule are as follows:

The responsible authority is required by the statute to identify, in the public document, all records, files, and processes maintained by the agency which contain private or confidential data. To be able to label certain data as private or confidential, the responsible authority must base his/her determination of data classification on a statute or federal law. The rule requires the responsible authority to identify those statutes or applicable provisions of federal law. By requiring the responsible authority to cite the authority for the determination, the rule fulfills two needs. First, this requirement provides a check on the responsible authority's use of discretion to classify data. If the responsible authority is properly determining data classification, he or she should be able to cite the authority for that determination in the public document.

Second, by requiring the responsible authority to cite the authority to classify specific data, the rule provides an additional check on administrative discretion. The general public and any individual data subject are provided with information by which they can, by examining the cited authority, decide for themselves whether the responsible authority has determined the proper classification for the data in question. This ability to independently evaluate the cited authority is particularly needed when the responsible authority has determined that the data in question is classified as confidential.

Section B. 2 and 3: Other than to identify the general contents of the public document, the Act provides few detailed specifications by which the responsible authority can be sure he or she has complied with the Act. The rule provides guidelines to the responsible authority against which compliance can be evaluated. The guidelines proposed by the rule will require the responsible authority to prepare a document that is understandable by the general public. This is necessary to assure that the public document does not become an exercise in "bureaucratese." To afford the opportunity for the greatest possible compliance, the rule also provides assistance to the responsible authority in the form of a sample public document set forth in an appendix to the rules.

2 MCAR § 1.215.DUTIES OF THE RESPONSIBLE AUTHORITY AS THEY RELATE TO THE ADMINISTRATION OF PRIVATE AND CONFIDENTIAL DATA

This rule deals with problems presented by the statutory requirement, particularly as set out in Section 15.1641, that different tasks be performed by the responsible authority depending on the classification of the data being administered. This rule elaborates on and clarifies the special tasks assigned to the responsible authority when the particular data is classified as either private or confidential.

Section A: To administer private or confidential data consistent with the provisions of Section 15.1641, it is an implicit requirement of the Act that the responsible authority first determine the lawfully authorized purposes for the collection, use, and dissemination of such data. The Act requires the responsible authority to make this determination in reference to two different time frames. The time frames for determining purposes are 1) prior to August 1, 1975, and 2) subsequent to August 1, 1975. Section A fulfills the need of explaining to the responsible authority how that determination is to be made and the consequences of the determination. The rule clarifies the varying requirements attached to data collected either before 1975 or after 1975.

Section B: This section fulfills the need of explaining to the responsible authority how the determination of purposes is made for post-1975 data. The current wording of the Act contemplates that since August 1, 1975, purposes for data collection have been communicated to data subjects as required by Section 15.165 of the Act. Experience with the Act makes it obvious that this communication has not been done by all agencies. This section deals with that additional problem by adopting a "should have" type of standard.

Section C: Having performed the preliminary task of determining purposes and uses, the responsible authority is prepared to comply with the detailed requirements of the Act. There has been much confusion concerning these particular requirements. This section

of the rule is proposed to eliminate that confusion. The rule does so by providing answers to the questions most asked about Section 15.1641 (c) of the Act. The section accomplishes this purpose in a reasonable fashion by translating the legal requirements of the Act into a proposed administrative method for compliance. This method revolves around preparation of a list identifying purposes and uses and utilization of that list in complying with the Act by performing various tasks required by the Act.

Section D: Section C is basically concerned with tasks to be performed by the responsible authority that related to persons outside the agency. Performance of these tasks will also have logical implications for the internal operation of the agency. Section D is concerned with detailing those internal tasks for the responsible authority. The general objectives of this section are to provide guidance so that personnel of the agency will be able to comply with the requirements of the Act.

Section E: Section 15.1641 (c) of the Act requires the responsible authority to comply with a requirement that private or confidential data only be administered for lawful purposes. However, the Act also provides certain discretion within which the responsible authority may change or establish new purposes, subject to certain requirements. This discretion is the subject of the latter part of Section 15.1641, Subdivision (c). Section E of this rule is necessary to provide the limits on the responsible authority's exercise of this discretion. The section also provides certain definitions that are necessary to the responsible authority's understanding of and administration of the Act. This is necessary because certain terms are not defined by the Act itself.

2 MCAR § 1.216. DUTIES OF THE RESPONSIBLE AUTHORITY AS THEY RELATE TO THE ADMINISTRATION OF ALL ENTITY DATA

The special limitations placed on the collection, use, and dissemination of private and confidential data are the subject of Rule § 1.215. The Act also places certain limitations on the collection and storage of all agency data. These limitations are the subject of Section 15.1641 (c) of the Act. The Act establishes a basic limitation that collection and storage of all agency data and the use and dissemination of the agency's private and confidential data is "...limited to that necessary to the administration and management of programs specifically authorized by the legislature, local governing body or mandated by the federal government. Rule § 1.216 is necessary to clarify the meaning of the quoted phrase and to provide direction to responsible authorities.

Clear direction is necessary because the statute is imposed on an administrative reality that for years has featured relatively

unrestrained data collection. Although the statutory direction is clear, the administrative implications of the plain words of the statute are not clear. Typical questions that are asked in this area are: 1) What is necessary data? 2) How do we determine if something is necessary? 3) What do we do if we determine something is not necessary? This rule has been written to provide answers to those questions among others and to give clear direction to responsible authorities concerning the administrative implications of the statutory section.

Section A: It is clear that the statute imposes a limitation on data practices relating to a "necessary" requirement. What is not clear is how the responsible authority determines whether the data maintained by his or her agency is "necessary to the administration and management..." of the agency's functions and programs. To provide a method of determination, the rule proposes that responsible authorities first determine what data is in use by their agencies. Following that determination, the rule requires responsible authorities to relate actual data usage to the usage specifically contemplated by either local, state, or federal enabling enactments.

To accomplish that requirement, and to assure compliance with the requirements contemplated by the Act, the rule proposes that a plan be developed by the responsible authority. Previous versions of this section, which explicitly laid out the detailed steps to be followed by the responsible authority in the determination of what is "necessary", were criticized during the IISAC review of the draft rules. (This was the review required by Section 15.1671.) The basis of the IISAC criticism was that this task was gigantic and probably beyond the resources of any responsible authority. In response to that criticism, the rule was redrafted in its present form which requires the responsible authority to develop a plan. Because the plan is developed by personnel of the agency itself, it should be uniquely adapted to the capabilities and problems present in each particular agency. This approach is more reasonable than to establish a rigid and detailed rule which may not be workable in the particular environment of each specific agency. By providing for a plan, the rule attempts to maximize the discretion afforded to the responsible authority in his/her attempts to comply with the general statutory requirements. However, the rule does provide certain guidelines within which the plan must be developed. These guidelines are necessary to assure that the general statutory requirements are met.

Section B: It has become a somewhat common practice for public administrators to assert that all that is required to comply with the statutory requirement it to assert, solely as an exercise in administrative discretion, that certain data is necessary. This is exactly the kind of discretion that this provision of the statute was intended to limit. In its formulation of the "necessary" requirement, the Act attempts to limit such unbridled discretion.

This section is necessary to clarify for the responsible authority the scope and nature of the limits on his or her discretion. Details of such limits must be set forth in the rule because such details are not found in the Act itself.

To work within the statutory limitations on what is "necessary" the responsible authority must determine what actually constitutes necessary data. The definition of the term "necessary" is not provided by the statute. Section B, in its entirely, is devoted to defining that term as it relates to the administration of governmental data.

Section C: It is implicit in the statute's "necessary" limitations that unnecessary data cannot be collected, stored, used, or disseminated. By requiring the responsible authority to determine what data is necessary, it is logical that the responsible authority will also determine that certain data is not necessary. This section is concerned with the actions that the responsible authority must take to properly dispose of any data determined to be not necessary. The rule is necessary to provide language and guidance to fill in the logical omission presented by the current words of the statute.

Section D: This section is concerned with the duties assigned to the responsible authority by subsection (e) of Section 15.1641 of the Act. The intent of the Act's section is clear in that it requires the responsible authority to assure that all data collected, used, and disseminated by the agency is (quoting the Act) "accurate, complete and current." What is not clear about the statutory section is the meaning of the quoted terms in the context of the overall objectives of the Act.

Section D fulfills the need of prescribing a set definition of those terms. Providing a standard definition for these terms will also fulfill the need of assuring that administrative practices concerning data are made more uniform across all agencies of the state. This imposition of uniformity is one of the rationales underlying the whole thrust of the Act.

2 MCAR § 1.217. DUTIES OF THE RESPONSIBLE AUTHORITY AS THEY RELATE TO COMPUTERIZED DATA

Section 15.1641 (e) of the Act makes it clear the security problems presented by computerized data should be of special concern to responsible authorities as they implement and administer the Act. Beyond expressing concern, the statute says nothing about how that concern is to be translated into positive administrative action by responsible authorities. The proposed rule fulfills this need by providing specific direction as to the steps that must be taken by the responsible authority to assure that computer data is maintained by the agency according to certain security requirements.

Section A: Tha Act limits the special emphasis on security arrangements to data maintained in "directly accessible files." To understand the duties under the Act, the responsible authority must understand the meaning of the quoted term. However, the Act does not define that term. The section fills this need by clearly defining the term "directly accessible files."

Sections B and C: Because there has been a general emphasis on data security requirements in recent years, most governmental data centers have security measures of varying quality in place. Because security measures are in place in computer facilities, it would be unreasonable to require agencies to start from scratch in establishing security measures. Section B. acknowledges this condition by proposing an audit of an entity's security as the starting point for compliance with the statute. The audit is proposed to consist of a review and evaluation of the agency's current security measures. Because of the variance in computerized systems and facilities, Section C. allows the extent and nature of the audit to be at the discretion of the responsible authority. However, the section does present certain requirements that must be a part of the audit. These requirements are proposed so that the responsible authority's discretion to conduct this audit is bound by some requirements.

Sections D and E: Depending on the responsible authority's assessment of the adequacy of the security measures currently in place in the agency, Section D. prescribes certain measures that must be taken if the responsible authority deems it necessary. Included in those measures are many of the commonly used data security techniques, whose objective is to minimize the risk of unauthorized access to data and data tampering. Becuase of the dynamic nature of computerized systems, including software and hardware developments, Section E. further requires auditing of security measures be a part of any agency's ongoing management of computerized data.

2 MCAR § 1.218. ADMINISTRATIVE APPEAL

Section A: The process of bringing an appeal from a determination of a responsible authority, a right conferred by Section 15.165, Subdivision 4, is generally regulated by the provisions of Chapter 15. of Minnesota Statutes and by rules promulgated by the Office of Hearing Examiners. This section of the rule acknowledges those requirements by referencing the other authority that guides the administrative appeal process.

Section B: The Act's handling of administrative appeals presents the need to describe the detailed administrative information necessary to bring the appeal. This section fills this need by providing addresses and certain other information for the content of the actual appeal documents.

Because the data in dispute may be classified as private, this section also provides for the ability to process the appeal under a pseudonym, instead of the real name of the data subject.

Section C: In initiating and maintaining any contested case to resolve a dispute brought to the Department pursuant to Section 15.165 of the Act, the Department will be acting as a neutral party in a quasi-judicial capacity. Compliance with the Administrative Procedures Act and the Rules of the Hearing Examiner will require the Dapartment to incur costs. The proposed rule Section is necessary to provide a means to bill those costs to the responsible authority whose data is in dispute. The proposed section is reasonable in that it assigns costs to the party who is in the best position to resolve the dispute at the earliest opportunity without resort to a contested case proceeding which may prove costly to all parties involved.

2 MCAR § 1.219. GENERAL POWERS OF THE COMMISSIONER

Section A: The enforcement powers of the Commissioner concerning the Act have been the subject of considerable discussion since the initial passage of the Act. This rule is necessary to define the Commissioner's power and authority. This section of the rule takes the position that a careful reading of the Act clearly establishes that the Commissioner's authority is limited. This section is necessary to describe the exact limits of the Commissioner's authority.

Sections B and C: There is no express authority for the establishment of a "Data Privacy Unit" expressed in the Act. Such a unit currently operates in the Department of Administration. The large volume of questions generated by the Act caused the Commissioner of Administration to create such a "unit" in 1974. Since that time the unit has functioned to provide a central place from which information concerning the Act can be provided to citizens and to administrative agencies. As the rules, once they are promulgated, will become a primary reference for responsible authorities and citizens, information concerning this information center's function should be made a part of the rules. For the rules not to acknowledge the existence of the Data Privacy Unit would be to ignore reality. It would also deprive agencies and citizens of a valuable source of information and assistance concerning the Act. These sections of this rule fulfill the need of providing information concerning the existence and location of the unit.

2 MCAR § 1.120. DUTIES OF THE COMMISSIONER RELATING TO THE EMERGENCY CLASSIFICATION OF DATA

This rule is necessary to provide some needed procedures and definitions that are not stated as a part of the emergency classification section of the Act, Section 15.1642.

Section A: Although the statutory section does provide general specifications of what must be contained in an application, the Act's provisions do not structure or format these specifications. This section of the rules addresses that problem by requiring responsible authorities to use a form provided by the Commissioner. That form, which has been prepared according to the requirements of Section 15.1642, is made a part of the Appendix to the rules.

Section B: There are a number of terms used in Section 15.1642 that are critical to an understanding of the section and of the process associated with the emergency classification of data. Several of the terms are not defined by the Act itself. This section of the rule fulfills the need of providing necessary definitions.

Section C: The Commissioner of Administration has delegated the preliminary work of screening and evaluating applications for emergency classification of data to the Data Privacy Unit. This section of the rule is necessary to provide time savings and to reduce administrative complications by guiding responsible authorities directly to the proper place for submitting applications.

Section D: The Act establishes what appear to be rigid time frames within which certain activities must be accomplished by the applicant and by the Department. In the experience of processing applications, it often occurs that an applicant has forgotten or omitted part of the information necessary to the processing of the application. To penalize the applicant by letting the time frames run while paperwork is being mailed back and forth would not be reasonable. This section of the rule is being proposed to take care of that problem by providing for the eventuality that a responsible authority must supplement an application with additional information.

Section E: Each legislative session it appears that the legislature may repeal the emergency classification authority given to the Commissioner. In the last three sessions, the legislature has chosen to extend that authority for one year only. Rule § 1.120. will have no meaning if the legislature repeals the emergency classification authority. This section is proposed to handle that situation by providing for a "repeal" of the rule in the event the underlying legislation is repealed.

2 MCAR § 1.221 SEVERABLE PROVISIONS

This section is a standard section for almost all rules proposed by administrative agencies. Its rationale is to provide for the severing off of any proposed rule found to be invalid during the hearing process.

Date: 10/5/78

Richard L. Brubacher
Commissioner

Police interpretation of privacy law brings charges of withholding data

Minneapolis Tribune - Sun., Jan. 11, 1976

By Jack Coffman
Staff Writer

Confusion over Minnesota's privacy laws has been growing in recent months, leading to accusations that officials are using the laws to withhold information.

The situation — subject of a legislative hearing Monday — has resulted, among other things, in:

■ The withholding for two days of the name of a suspect arrested in a college bomb threat.

■ The refusal of a city council to indentify candidates for a top municipal job. When the council mentioned the candidates in public meetings, they were referred to only by number.

■ The policies of some counties of keeping the names of people arrested confidential until formal charges have been filed, sometimes days after the arrest.

Officials say the privacy laws prevent them from divulging such information, for, if they did, they might be sued by the people identified. Critics of such policies, primarily in the news media, say the situation results in a system of "secret arrests."

State Sen. Robert Tennessen, chairman of the Senate Judiciary Subcommittee on Privacy, said he is concerned about confusion over the

Privacy continued on page 8A

Privacy

Continued from page 1A

law.

"There is no basis for having secret arrests in Minnesota," the Minneapolis DFLer said.

The law was intended to prevent large-scale collection of secret data on individuals by government agencies. It was amended this year in an effort to protect the confidentiality of investigations in the attorney general's office. The wording of the change, however, has been interpreted by some law-enforcement officers as a prohibition against releasing information to the press.

The legislative hearings are expected to produce an airing of the positions on both sides of the issue. Law-enforcement officers and news-media officials are scheduled to testify in the hearings, which will begin at 10 a.m. in Room 118 at the Capitol.

Tennessen said there have been several reports from the Twin Cities and outstate areas that law officers are treating the identities of arrested people as confidential because of the state law. Critics say that this could result in someone being held in jail for 36 hours (after which a charge must be made) and that, during that period, it would be impossible to determine the identity of the person being held.

Last week a woman was arrested in Marshall on a complaint stemming from an alleged bomb threat against Southwest State University. Police refused to release her name to the Marshall Independent, contending that the privacy law prevented such disclosure. Although the woman was arrested on Monday and released on bond, the newspaper was not given her name until Wednesday, when she was arraigned in court.

The privacy law also was used in Marshall recently to conceal the identities of candidates for the job of city administrator. During discussion of the merits of the candidates in public the council only referred to them by a number, not by name.

City Attorney Joseph Bot said the privacy law was used to shield the three final candidates' identities because they requested that confidentiality and because naming them might hurt their present job status. In contrast, the names of candidates for superintendent of Minneapolis schools were made public.

"Just because they are applying for a public job, does that mean they open themselves up?" Bot asked.

Other officials say the changes in the privacy laws have changed the way they treat information. Donald Eustice, Waseca County sheriff, said the law prevents him from releasing the names of people arrested until they are actually charged. He acknowledged that under this system someone could be held in jail and no one outside the legal system would be able to find out. However, he said, someone might be arrested and later it would be determined there was no case against the person. Then, he said, "we might be in real trouble."

Until the change in the law, the St. Paul Police Department revealed the names of those arrested. It has since reversed that policy because of an interpretation of the privacy laws by the city attorney's office.

In addition, news media were denied access to investigation reports that had been available before. The St. Paul Dispatch and Pioneer Press sought to overturn this policy change in court. Judge Joseph Summers, in a move that did not rule on the newspaper petition, urged his fellow judges to approve a court rule that investigation reports on misdemeanor and petty-misdemeanor charges be made available to reporters. Most judges agreed.

In Hennepin County the daily roster of inmates at the county jail is kept confidential by Sheriff Donald Omodt.

His position is that law officers did not ask for the law in the first place, but that now that they are faced with it, they must abide by it strictly.

"If they (legislators) want to change it, it's fine with us," Omodt said.

Privacy continued on page 9A

ATTACHMENT # 1

Privacy

Continued from page 8A

Chief Deputy W. R. Hoagland said one out of four people brought to the jail is subsequently released with no immediate charge filed. He feels keeping these names confidential is consistent with the spirit of the privacy laws.

"If a law enforcement officer bends over backwards to see that the name of a person arrested but later not charged isn't plastered all over the newspaper, it seems to me we are following the intent of the law," he said.

Paul Tschida, superintendent of the Bureau of Criminal Apprehension (BCA), said he feels that some law officers are now concerned about what could happen to them if they reveal information considered confidential under the privacy law.

"What they are scared about is that if they do release it, someone will sue them," said Tschida. "So if you do nothing, at least you are safe."

John Meyer, Detroit Lakes publisher and president of the Minnesota Newspaper Association, has said that in some counties "we now have secret arrest and incarceration until the time of arraignment. We do not believe the Legislature or the people of this state will allow for such a situation to continue, and we call for action as quickly as possible to end this trend."

Robert Shaw, lobbyist for the association, said, "The law is being misinterpreted all over the place."

Early last week a slightly different situation arose involving the refusal to divulge the name of an accused, this time a person who had been arraigned on kidnap charges in Benton County.

Judge Paul Doerner, at the request of Benton County Attorney Richard Jessen, ordered all officials under his jurisdiction not to make the name available to reporters. The ban was also directed at representatives of the news media in the courtroom; since there were none there, the impact of the ban was questionable.

However, the suspect was also charged in Sherburne County, where there was no embargo on his identity.

The name of the suspect was printed in many papers that day, leaving Jessen, who had wanted to avoid pretrial publicity, wondering, "It turns out to be a mess, and at this point, I'm not sure it was worth it."

And, in discussing the situation by telephone last week, Judge Doerner requested that he not be identified in the story about the order.

ATTACHMENT # 1

ATTACHMENT # 1

Panel to attempt privacy-law change

By David Kuhn
Staff Writer

Members of a state Senate subcommittee agreed Monday to attempt to draft legislation to resolve a dispute between some law-enforcement agencies and news organizations over the disclosure of certain arrest data.

Testimony before the subcommittee yesterday underscored, however, the difficulties of satisfying both law enforcement and news media officials, who have basic differences on the issue.

The conflict focuses on whether the identities of people arrested but not yet charged should be available as public information, and whether the state's public-records law does or does not permit release of that information now.

Until late last year, when the state's privacy act was revised, disclosure of arrest data was governed only by the broadly worded Public Records Act and by varying interpretations given to it by law-enforcement agencies.

The 1975 amendments removed an exemption covering criminal-investigation data and made law-enforcement officials subject to penalties contained in the privacy act for violation of that law. The penalties can include suspension without pay or loss of job.

Sen. Robert Tennessen, DFL-Minneapolis, the subcommittee chairman, said yesterday that the privacy-law revision was not intended to have any effect on the Public Records Act. Any information previously made available should still be available, he said.



State Sen. Robert Tennessen

But the issue arose when police officials and city or county attorneys in some jurisdictions, including St. Paul, interpreted the privacy act to mean that identities of people arrested "for probable cause" but not charged must be withheld or the officials involved would be liable to the penalties.

Spokesmen for the Minnesota Joint Media Committee, an umbrella group of the state's news media, submitted proposed changes in the laws.

John Finnegan, executive editor of the St. Paul Dispatch and Pioneer Press, said withholding of the identities of arrested people makes it possible for police to make secret arrests and hold citizens for up to 36 hours before releasing them or charging them.

"It is essential in our democratic society that the public, through its representatives in the media, be able to monitor the activities of the police," Finnegan said.

Several news spokesmen said police, who have the power to invade a person's privacy by arresting him, should not have the power to decide whether to disclose that information.

Law-enforcement officials disagreed totally. They said it would be an unwarranted invasion of individual privacy to disclose the names of people arrested but not charged. They also discounted the likelihood of secret arrests if identities were not made known before charges were filed. Nevertheless, they agreed that the laws should be clarified.

Minneapolis Tribune 7B
Tues., Jan. 13, 1976

ATTACHMENT # 2

DFL-Minneapolis

A Guest Column

Editor's note: The Star, with the help of Sen. Tennessen, asked a number of experts on the privacy issue to write guest columns. Their contributions will follow this first column by Tennessen. Minn Star 2/16/74

Privacy is a fundamental right necessary to maintain human dignity and to preserve a free and democratic society. No one whose beliefs, thoughts, ideas and lawful deeds have been exposed for the whole world to see without his consent can be free. Yet the unabated collection and disclosure of personal data by government has interfered with this fundamental right of many.

Alexander Solzhenitsyn eloquently illustrated in "Cancer Ward" the severe limitations on actual freedom as well as on a person's sense of freedom which necessarily and inevitably result from unrestrained governmental intrusion into one's personal life. The tyranny thus exercised over individuals is no less real when the invasion of privacy is by private individuals or by the press.

The need for privacy has recently attained a new urgency because of governmental intrusion into the private lives of citizens. Watergate, U.S. Army surveillance of civilians lawfully exercising their political rights, and illegal FBI surveillance have illustrated the need for specific legislative guarantees to protect a person's privacy. The protection must prevent excessive intrusion into a person's beliefs, thoughts, ideas and lawful activities which the person has not chosen to share with others. Protection must also be afforded to personal information we voluntarily share with others for a specific purpose to prevent unauthorized use for other purposes or by third persons.

Invasion of man's privacy and subsequent exposure or mere threat of exposure is a means of control designed to stifle dissent, unconventional thoughts, beliefs and ideas as well as lawful actions. Some protection against governmental interference is found in the Fourth and Fifth Amendments to the U.S. Constitution. The Fourth protects "the right of people to be secure, in their persons, houses, papers and effects, against unreasonable search and seizure" while the Fifth protects us in criminal cases from having to be witnesses against ourselves. Certainly privacy is a right as equally important to a free democratic society as is a free press.

Both privacy and freedom of press are fundamental rights. At times they may conflict. A free press is necessary to guard against incompetency and corruption in government by informing the public. In a free democratic society, government is possible only with the informed consent of the governed. However, not all personal information the government collects is or should be public. We have protected the confidentiality of tax returns and adoption records. Classification of data involves the balancing of the rights of privacy and a free press. If public, the information must be available to the most humble citizen on the same basis as to the most powerful newspaper. No greater right to know exists in the latter.

Minnesota has long had a public records law requiring public officials to keep all records necessary to the exercise of their duties and to make the records available for public inspection at reasonable times, subject to some statutory exceptions. The law has not been recently changed.

Government has long collected more personal data than is necessary to carry out its statutory and constitutional duties. Although the information gathered has often been inaccurate, nevertheless it has been the basis for denying citizens certain benefits. Also, even though collected for one purpose, the personal data has a potential to be used for other purposes without that person's consent. First in the nation, Minnesota in 1974 adopted a privacy act to protect citizens' right to privacy. The act was amended in 1975.

The Privacy Act restricts collection of personal data to that necessary to carry out duties mandated by legislation, ordinances and executive orders. It greatly restricts use of information for purposes other than that for which collected; it gives citizens the right to examine records about themselves and the means to correct inaccuracies; and it ensures that no data banks whose existence is secret will exist.

The definition of a public record was not altered by the Privacy Act. Rather, it incorporated the definition by specific reference. Recently various police departments have refused to disclose the names of persons arrested or held, ostensibly on the basis of the Privacy Act. However, when pressed on the point in a public hearing, the St. Paul city attorney claimed his opinion was based upon his interpretation of the public records law and in no way upon the Privacy Act itself.

I do not believe secret arrests or jailings can be based upon either statute. Any police department withholding the names of those arrested is violating the public records law. St. Paul's claim is only a new wrinkle in an old issue. Prior to the 1974 act, the Minneapolis Police Department at one time refused to disclose the names of those arrested, claiming that it was protecting their privacy.

I think the issues of secret arrests are clear. Secret arrests are the hallmark of a totalitarian society. The potential for corruption and illegal police activity must be prevented by continuing to treat the names of persons arrested as public. In balancing the rights of privacy and the right of a free press, the protection of a free and democratic society is better maintained by public disclosure of names of persons arrested.

Clearly, a right to privacy is an essential component of a free society. Clearly, a vigorous free press is no less essential. What happens when these fundamental essentials come into conflict is not so clear. Minnesota's Privacy Act is an attempt to guard privacy and to provide some guidance in conflicting situations.

RECEIVED
OCT 30 1978
ATTORNEY GENERAL
ADMINISTRATIVE AGENCIES

Sheila -
I did not make copies of the comments for you. If you want them, please yell.
- D -

STATE OF MINNESOTA

DEPARTMENT OF ADMINISTRATION

IN THE MATTER OF THE PROPOSED ADOPTION OF RULES OF THE DATA PRIVACY UNIT GOVERNING THE ENFORCEMENT AND ADMINISTRATION OF THE "MINNESOTA DATA PRIVACY ACT"

MATERIALS RECEIVED AFTER GIVING NOTICE OF INTENT TO SOLICIT OUTSIDE OPINION

On June 5, 1978, the Data Privacy Unit of the Department of Administration gave notice in the State Register of its intent to solicit outside opinion on the proposed rules governing the enforcement and administration of the "Minnesota Data Privacy Act." This notice appeared in the State Register, Volume 2, Number 48, June 5, 1978, at page 2167.

Following that notice, materials expressing opinion were received from individuals, agencies and associations outside of the Department of Administration. Copies of all materials received are attached.

Date: October 4, 1978

Donald A. Gemberling

Donald A. Gemberling
Manager, Data Privacy Unit
Department of Administration

Attorney General

Don Gemberling
Data Privacy Unit

July 18, 1978

Sheila S. Fishman
Special Assistant
Attorney General

296-6204

Draft 10 and Comments

ADM/DPU2H.2. - Page 7

Towns-It is possible that the reference to towns was omitted from the previous law because it was redundant and was included in the broad terminology of Subd. 5. Minn. Stat. § 379.01 describes how a town is created pursuant to law.

Is a town listed as a political subdivision for purposes of notice?

ADM/DPU2L.2.d.

Is it possible that a non profit corporation or agency could also be a statewide system? If so, you probably should indicate whether the procedures described in 2. or 3. prevail. If 2., say something to that effect (example: If the corporation or agency is a statewide system, this section shall be applicable and...) and incorporate D. Olson's suggested language.

ADM/DPU3.A. - PAT HIRL'S COMMENTS

I like Pat Hirl's suggestion regarding time but think it is not a good idea to list a specific number of days--especially 5. Can you include a #2 providing that the RA shall comply within a reasonable time.

I am not particularly convinced of the necessity for revisions suggested in #7.

ADM/DPU4.-A.2.

I do not think a specific authorization is required (much too burdensome on the R.A.) but I would agree to rewriting 2 so that it is a little tighter. Perhaps---

2. **Individuals within the entity whose work assignment reasonably requires access.**

ADM/DPU18 - page 35

Minn. Stat. § 15.052, subd. 6 gives the Hearing Examiner the authority to access costs to state agencies. This, together with the fact that there is no statutory authority to pass the cost back, will make subd. C hard to get through. I agree, that we should try.

SSF:mb

Data Privacy Unit
Dept. of Administration
2nd Floor
State Administration Bldg.
St. Paul, MN 55155
(612) 296-6729 or
296-6733

County Attorneys Council
40 North Milton
St. Paul, MN 55104
(612) 296-6972

April, 1978

OFFICIAL RECORDS

COLLECTION, SECURITY AND

DISSEMINATION OF DATA

Minnesota Statutes 15.162 to 15.1671 are provided as amended by the 1978 Legislature in Chapter 790 (H. F. 2466). All 1978 amendments are effective April 6, 1978.

The format for the following is:

a. New 1978 language - <u>underlined</u>.

b. Language struck by the 1978 amendments - lined out, for example: ~~the date~~.

c. Language not changed by the 1978 amendments - plain type.

Minnesota Statutes 15.17 to 15.174 are provided for your information. Minnesota Statutes 15.169 has been omitted because the Privacy Study Commission's statutory existence expired in January, 1977.

NOTE: This booklet contains an unofficial copy of Minnesota's Data Privacy Act and Official Records Act. Questions or problems which arise under these laws may be directed to the State Data Privacy Unit at the above address.

15.162 COLLECTION, SECURITY AND DISSEMINATION OF RECORDS; DEFINITIONS.

Subdivision 1. As used in sections 15.162 to 15.1671 the terms defined in this section have the meanings given them.

Subd. 1a. "Arrest information" shall include (a) the name, age, and address of an arrested individual; (b) the nature of the charge against the arrested individual; (c) the time and place of the arrest; (d) the identity of the arresting agency; (e) information as to whether an individual has been incarcerated and the place of incarceration. "Arrest information" does not include data specifically made private, confidential or nonpublic pursuant to section 260.161 or any other statute.

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

Subd. 2a. "Confidential data on individuals" means data which is: (a) made not public by statute or federal law applicable to the data and is inaccessible to the individual subject of that data; or (b) collected by a civil or criminal investigative agency as part of an active investigation undertaken for the purpose of the commencement of a legal action, provided that the burden of proof as to whether such investigation is active or in anticipation of a legal action is upon the agency. Confidential data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration. The provision of clause (b) shall terminate and cease to have force and effect with regard to the state agencies, political subdivisions, statewide systems, covered by the ruling, upon the granting or refusal to grant an emergency classification pursuant to section 15.1642 of both criminal and civil investigative data, or on July 31, ~~1978~~ 1979, whichever occurs first.

Subd. 3. "Data on individuals" includes all records, files and processes which contain any data in which an individual is or can be identified and which are retained or intended to be retained on a permanent or temporary basis. It includes data collected, stored, or disseminated by manual, mechanical, electronic or any other means. Data on individuals are classified as public, private or confidential.

Subd. 4. "Individual" means a natural person. In the case of a minor, "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. 5. "Political subdivision" means any county, statutory or home rule charter city, school district, special district and any board, commission, district or authority created pursuant to law, local ordinance or charter provision. It includes any nonprofit corporation which is a community action agency organized pursuant to the economic opportunity act of 1964 (P. L. 88-452) as amended, to quality 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. 5a. "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. Private data on individuals does not include arrest information that is reasonably contemporaneous with an arrest or incarceration.

Subd. 5b. "Public data on individuals" means data which is accessible to the public in accordance with the provisions of section 15.17.

Subd. 6. "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 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 or summary data, unless otherwise provided by state law.

Subd. 7. "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. 8. "Statewide system" includes any record-keeping system in which data on individuals 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. 9. "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.

15.163 REPORTS TO THE LEGISLATURE.

Subdivision 1. On or before August 1, 1976, the responsible authority shall prepare a public document containing his 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 his state agency, statewide system, or political subdivision. 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 keep it accurate.

Subd. 2. 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.

15.1641 DUTIES OF RESPONSIBLE AUTHORITY.

(a) Data on individuals is under the jurisdiction of the responsible authority who may appoint an individual to be in charge of each file or system containing data on individuals.

(b) Collection and storage of public, private or confidential data on individuals and 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, local governing body or mandated by the federal government.

(c) Private or confidential data on individuals shall not be used, collected, stored or disseminated for any purposes other than those stated to an individual at the time of collection in accordance with section 15.165 or, in the case of data collected prior to August 1, 1975, for any purpose other than those originally authorized by law, unless (1) the responsible authority files a statement with the commissioner describing the purpose and necessity of the purpose with regard to the health, safety or welfare of the public and the purpose is approved by the commissioner, or (2) the purpose is subsequently authorized by the state or federal legislature, or (3) the purpose is one to which the individual subject or subjects of the data have given their informed consent.

(d) The use of summary data derived from private or confidential data on individuals under jurisdiction of one or more responsible authorities shall be permitted, provided that summary data is public pursuant to section 15.17. The responsible authority shall prepare summary data from private or confidential data on individuals upon the request of any person, provided that the request is in writing and the cost of preparing the data is borne by the requesting person. The responsible authority may delegate the power to prepare summary data to the administrative officer responsible for any central repository of summary data, or to a person outside of its agency if the person agrees in writing not to disclose private or confidential data on individuals.

(e) The responsible authority shall establish procedures and safeguards to ensure that all public, private

or confidential data on individuals is accurate, complete and current. Emphasis shall be placed on the data security requirements of computerized files containing private or confidential data on individuals which are accessible directly via telecommunications technology, including security during transmission.

15.1642 EMERGENCY CLASSIFICATION.

Subdivision 1. APPLICATION. The responsible authority of a state agency, political subdivision or statewide system may apply to the commissioner for permission to classify data or types of data on individuals as private or confidential, for its own use and for the use of other similar agencies, political subdivisions or statewide systems on an emergency basis until a proposed statute can be acted upon by the legislature. The application for emergency classification is public.

Upon the filing of an application for emergency 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 30 days, or until the application is disapproved or granted by the commissioner, whichever is earlier.

Subd. 2. CONTENTS OF APPLICATION. An application for emergency classification shall include and the applicant shall have the burden of clearly establishing at least the following information:

(a) That no statute currently exists which either allows or forbids classification as private or confidential;

(b) That data similar to that for which the emergency classification is sought has been treated as either private or confidential by other state agencies or political subdivisions, and by the public; and

(c) That a compelling need exists for immediate emergency 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. The commissioner shall either grant or disapprove the application for emergency classification within 30 days after it is filed. If the commissioner disapproves the application, he shall set forth in detail his reasons for the disapproval, and shall include a statement of what classification he believes is appropriate for the data which is the subject of the application. Ten 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 on individuals, unless the responsible authority submits an amended application for emergency classification which requests the classification deemed appropriate by the commissioner in his 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 15 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 15 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 appli cation shall become public data on individuals. No more than one amended application may be submitted for any single file or system which contains data on individuals.

If the commissioner grants an application for emergency 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 20 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 4. All applications for emergency classification which are pending on the effective date of this section shall be deemed to have been filed on the effective date of this section.

Subd. 5. EXPIRATION OF EMERGENCY CLASSIFICATION. All emergency classifications granted under this section and still in effect shall expire on July 31, ~~1978~~ 1979. No emergency classifications shall be granted after July 31, ~~1978~~ 1979.

15.165 RIGHTS OF SUBJECTS OF DATA.

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

Subd. 2. An individual asked to supply private or confidential data concerning himself shall be informed of: (a) the purpose and intended use of the requested data within the collecting state agency, political subdivision or statewide system; (b) whether he may refuse or is legally required to supply the requested data; (c) any known consequence arising from his 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.

Subd. 3. Upon request to a responsible authority, an individual shall be informed whether he is the subject of stored data on individuals, and whether it is classified as public, private or confidential. Upon his further request, an individual who is the subject of stored private data on individuals shall be shown the data without any charge to him and, if he desires, 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 him for six months thereafter unless a dispute or action pursuant to this section is pending or additional data on the individual has been collected. The responsible authority shall provide copies of the private data upon request by the individual subject of the data. The cost of providing copies shall be borne by the individual.

The responsible authority shall comply immediately, if possible, with any request made pursuant to this subdivision, or within five days of the date of the request,

excluding Saturdays, Sundays and legal holidays, if immediate compliance is not possible. If he cannot comply with the request within that time, he shall so inform the individual, and may have an additional five days within which to comply with the request, excluding Saturdays, Sundays and legal holidays.

Subd. 4. An individual may contest the accuracy or completeness of public or private data concerning himself. 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: (a) 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 (b) notify the individual that he 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.

15.166 CIVIL PENALTIES.

Subdivision 1. Notwithstanding section 466.03, a political subdivision, responsible authority or state agency which violates any provision of sections 15.162 to 15.1671 is liable to a person who suffers any damage as a result of the violation, and the person damaged may bring an action against the political subdivision, responsible authority or state agency to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, the political subdivision or state agency shall, in addition, be liable to exemplary damages of not less than $100, nor more than $1,000 for each violation. The state is deemed to have waived any immunity to a cause of action brought under sections 15.162 to 15.1671.

Subd. 2. A political subdivision, responsible authority or state agency which violates or proposes to violate sections 15.162 to 15.1671 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 sections 15.162 to 15.1671.

Subd. 3. 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.

15.167 PENALTIES.

Any person who willfully violates the provisions of sections 15.162 to 15.1671 or any lawful rules and regulations promulgated thereunder is guilty of a misdemeanor. Willful violation of sections 15.162 to 15.1671 by any public employee constitutes just cause for suspension without pay or dismissal of the public employee.

15.1671 DUTIES OF THE COMMISSIONER.

The commissioner shall with the advice of the intergovernmental information services advisory council promulgate rules, in accordance with the rule-making procedures in the administrative procedures act which shall apply to state agencies, statewide systems and political subdivisions to implement the enforcement and administration of sections 15.162 to 15.169. The rules shall not affect section 15.165, relating to rights of subjects of data, and section 15.169, relating to the powers and duties of the privacy study commission. 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 15.0412, subdivision 3, of the date and place of hearing, enclosing a copy of the rules and regulations to be adopted.

15.17 OFFICIAL RECORDS.

Subdivision 1. MUST BE KEPT. All officers and agencies of the state, and all officers and agencies of the counties, cities and towns, shall make and keep all records necessary to a full and accurate knowledge of their official activities. All such public records shall be made on paper of durable quality and with the use of ink, carbon papers, and typewriter ribbons of such quality as to insure permanent records. Every public officer, and every county officer with the approval of the county board, is empowered to record or copy records by any photographic, photostatic, microphotographic, or microfilming device, approved by the Minnesota historical society, which clearly and accurately records or copies them, and such public officer or such county officer may make and order that such photographs, photostats, microphotographs, microfilms, or other reproductions, be substituted for the originals thereof, and may direct the destruction or sale for salvage or other disposition of the originals from which the same were made. Any such photographs, photostats, microphotographs, microfilms or other reproductions so made shall for all purposes be deemed the original recording of such papers, books, documents and records so reproduced when so ordered by any officer with the approval of the county board, and shall be admissible as evidence in all courts and proceedings of every kind. A facsimile or exemplified or certified copy of any such photograph, photostat, microphotograph, microfilm, or other reproduction, or any enlargement or reduction thereof, shall have the same effect and weight as evidence as would a certified or exemplified copy of the original.

Subd. 2. RESPONSIBILITY FOR RECORDS. The chief administrative officer of each public agency shall be responsible for the preservation and care of the agency's public records, which shall include written or printed books, papers, letters, contracts, documents, maps, plans, and other records made or received pursuant to law or in connection with the transaction of public business. It shall be the duty of each such agency, and of the chief administrative officer thereof, to carefully protect and preserve public records from deterioration, mutilation, loss, or destruction. Records or record books may be repaired, renovated, or rebound when necessary to preserve them properly.

Subd. 3. DELIVERY TO SUCCESSOR. Every legal custodian of public records, at the expiration of his term of office or authority, or on his death his legal representative, shall deliver to his successor in office all public records in his custody; and the successor shall receipt therefor to his predecessor or his legal representative and shall file in his office a signed acknowledgement of the delivery. Every public officer shall demand from his predecessor in office, or his legal representative, the delivery of all public records belonging to his office.

Subd. 4. ACCESSIBLE TO PUBLIC. Every custodian of public records shall keep them in such 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. Except as otherwise expressly provided by law, he shall permit all public records in his custody to be inspected, examined, abstracted, or copied at reasonable times and under his supervision and regulation by any person; and he shall, upon the demand of any person, furnish certified copies thereof on payment in advance of fees not to exceed the fees prescribed by law. 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 public records except as otherwise expressly provided by law.

15.171 OFFICIAL RECORDS; COMPILATION, MAINTENANCE AND STORAGE OF INFORMATION.

Notwithstanding any other law, any public officer who has jurisdiction over a collection of official records may select and use, subject to the approval of the commissioner of administration, alternative methods for the compilation, maintenance and storage of the information contained in those records, subject to the following conditions:

(1) The methods selected must provide for access to the information contained in the records by those authorized by law to have access to that information; and

(2) The methods selected must provide for the preservation of the information contained in the records to the extent specified by law.

15.172 APPROVAL OF ALTERNATE METHOD.

At least 90 days prior to the date upon which he proposes to put into effect an alternate method of compilation, maintenance, and storage of records, the public official shall submit a description of the proposed method and the reasons for adopting it to the commissioner of administration. If the commissioner of administration finds that the proposed method complies with the conditions specified in section 15.171, he shall approve its use; if not, he shall disapprove its use. A failure of the commissioner of administration to act before the date upon which the public official proposes to put the alternative method into effect shall be deemed a disapproval of that method.

15.173 NOTICE OF ALTERNATIVE METHOD.

Whenever the commissioner of administration approves an alternate method of compilation, maintenance and storage, he shall maintain a written notice of that approval, the date of taking effect of the alternate method, a description of the method and the reasons for its adoption in his office as a public record. In the case of a record having less than statewide significance, the public official having jurisdiction over the records shall file a written notice containing the same information as the notice maintained by the commissioner of administration with the county auditor, clerk or other similar recording officer of the affected governmental subdivision and such notices shall also be maintained as public records.

15.174 RECORDS NOW IN USE

Notwithstanding section 15.171, any public official using an alternate method of compilation, maintenance and

storage of a record on August 1, 1974, may continue to use that alternate method unless and until that method is expressly disapproved by the commissioner of administration. Such an official shall file a description of the method and the reasons for its use on or before August 1, 1974. Failure of the commissioner of administration to approve or disapprove such a method within 90 days shall be deemed an approval. Notice of such methods shall be filed as required in section 15.173.

NOTE: The following section was added to the Data Privacy Act by the 1978 Legislature. However, this section will not become effective until April 1, 1980.

15.1643 INTERNATIONAL DISSEMINATION PROHIBITED.

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.

Attorney General

Don Gemberling, Director
Data Privacy Unit

May 15, 1978

Sheila S. Fishman
Special Assistant
Attorney General

296-6204

Data Privacy Rules - Statement of Need

Following are comments on the proposed Rules and Statement of Need:

(a) The Statement of Need should demonstrate not only the need for the rules, but their reasonableness as well. Keep this in mind as you make revisions.

(b) If the Statement of Need does not refer to every provision and subject in your rules, there may be nothing in the record to support the rule and it may fall. So, even if you say, "It is needed for clarity" you have said something. However, it is better to say why it is needed for clarity.

(c) Include references to the statute (you do this frequently) as often as possible to show that you have statutory authority and are within the scope of the statute (on content, especially).

(d) Offer something supporting why a rule is mandatory or discretionary.

(e) I believe you can refer to types of questions asked or problems that arise to explain why a rule is needed. This will also tend to show your extensive experience with the rules.

(f) In instances where you repeat the statute offer some statement of why you feel it is necessary to do so.

(g) Even in sections that I think are good, feel free to expand on any point within your good judgment.

(h) Even after reading the Statement of Need, I am still uncomfortable with many of the provisions in the final sections of your rules. I think your devotion to telling others how to do their job is not proper subject for rules since it has no reasonable relationship to statutory purposes.

(i) Be certain to include some justification for all forms. You need more justification for mandatory forms than discretionary ones.

Please check the Statement of Need itself for additional comments. Also, I made a few comments on the rules although I think you did a good job and they are basically ready to go.

SSF:mb

2 MCAR § 1.201. Scope and purpose. These rules relate to and shall apply to the provisions of Minn. Stat. §§ 15.162 through 15.1671.

A. These rules shall apply to those governmental entities as defined by Minn. Stat. § ~~15.1671~~ 15.162, subd. 5, 7, and 8, which collect, create, use, store, and disseminate data on individuals as defined in Minn. Stat. § 15.162, subd. 3.

1. These rules shall only apply to data on individuals, as defined by Minn. Stat. § 15.162, subd. 3.

B. Non-profit social service agencies meeting the requirements of Minn. Stat. § 15.162, subd. 5 shall include, but are not limited to, agencies providing mental health, physical health, counseling and day-activities services.

1. These rules shall only apply in the instance where such an agency is required, by the terms of a written contract with a state agency, political subdivision, or statewide system to collect, create, store, use, or disseminate data on individuals.

2. In the event of such a contract, these rules shall only apply to the data on individuals that is actually generated by the social service agency because of the contract.

3. Any data generated by activities of the social service agency that are independent of the contractually based activities shall not be subject to these rules.

4. These rules shall not apply to personnel data maintained on employees of such social service agencies.

C. These rules shall not apply to any governmental data collected, created, used, stored, or disseminated which is not data on individuals as defined in Minn. Stat. § 15.162, subd. 3, except these rules shall apply to summary data.

D. Nothing in these rules shall limit the discovery procedures available at law to any party in a civil or criminal action or administrative proceeding as described in the Minnesota Rules of Civil Procedure and the Minnesota Rules of Criminal Procedure as adopted by the Minnesota Supreme Court or in Minnesota Statutes, and rules adopted thereunder.

E. Nothing in these rules shall restrict or limit the scope or operation of any judicial order or rule issued by a state or federal court.

1. In the event of the issuance of a subpoena duces tecum for any private or confidential data or a subpoena requiring any entity agent to testify concerning any private or confidential data, the court's attention should be called, through the proper channels, to those statutory provisions, rules, or regulations which restrict the disclosure of such information.

F. Nothing in these rules shall be construed to diminish the rights conferred on subjects of data by Minn. Stat. § 15.165, or any other statute.

G. The purpose of these rules is to aid governmental entities in implementing and administering Minn. Stat. §§ 15.162 through 15.1671~~.~~, as those sections relate to data on individuals. These rules are intended to guide entities so that while protection is given to individual privacy, neither necessary openness in government nor the orderly and efficient operation of government is curtailed.

2 MCAR § 1.202. Definitions. All terms shall have the meanings given them by Minn. Stat. § 15.162. Those terms and additional terms as used in these rules shall have the meanings as follows:

A. Act means Minn. Stat. §§ ~~15.162~~ 15.1611 through ~~15.1671~~ 15.1698, as amended, ~~commonly referred to as the "Data Privacy Act" or the "Minnesota Fair Information Practices Act"~~. officially entitled the "Minnesota Government Data Practices Act".

B. Arrest Information means only those elements of data that are expressly listed in § 15.162, subd. 1a of the Act. Arrest information shall only include data which is collected, created, or maintained by an entity whose officers, employees, or agents are given arrest powers by statute, or the power to take into custody any person arrested by another citizen of this state.

1. Such entities include, but are not limited to, municipal police departments, county sheriff departments, the Minnesota State Patrol, and officers deputized as game wardens under the provisions of Minn. Stat. § 97.50.

C. Data means "data on individuals" as defined in § 15.162, subd. 3 of the Act, unless stated otherwise.

1. Data can be maintained in any form, including, but not limited to, paper records and files, microfilm, computer medium, or other processes.

2. The duration of the existence of data, including whether certain data is temporary rather than permanent, is not relevant to compliance with these rules.

3. All data, in whatever form it is maintained, is "data on individuals" if it can in any way identify <u>any particular</u> a ~~unique~~ individual.

~~4. Code numbers representing unique individuals in certain data constitute "data on individuals", provided a list or index of any type is made available by which the code number can be cross referenced to identify unique individuals. Such data may qualify for treatment as summary data, pursuant to 2 MCAR § 1.209.~~

<u>4. Code numbers, which are used to represent particular individuals, constitute "data on individuals" if a list or index of any type is available by which the code number can be cross-</u>

referenced to a name or other unique personal identifier so that any individual's identity is revealed. Code numbers, lists of code numbers or data associated with code numbers may qualify for treatment as summary data, pursuant to 2 MCAR § 1.209.

a. Code number means the labeling or enumeration of data by use of a letter, number, or combination thereof, which is used in place of an individual's name, including but not limited to index numbers, dummy numbers, SOUNDEX codes, and social security numbers.

5. Data is "data on individuals" if it identifies an individual in itself, or if it can be used in connection with other data elements to uniquely identify an individual. Such data shall include, but is not limited to, street addresses, job titles and so forth where the particular data could only describe or identify one individual.

D. Confidential Data, as defined in § 15.162, subd. 2a of the Act, shall only include data which is expressly classified as confidential by either a state statute, including the provisions of § 15.1642 of the Act, or federal law.

1. Data is confidential only if a state statute or federal law provides substantially that:

a. Certain data shall not be available either to the public or to the data subject; or

b. Certain data shall not be available to anyone for any reason except agencies which need the data for agency purposes.

c. Certain data shall be confidential if a state statute or federal law provides that the data may be shown to the data subject only at the discretion of the person holding the data, and if such state statute or federal law provides standards which limit the exercise of the discretion of the person maintaining the data.

2. Data is not confidential if:

a. A state statute or federal law provides that the data is confidential, but the context of the statute or federal law, in which the term confidential appears, reasonably indicates the data is accessible by the data subject, or if the data subject is given access to the data only upon the discretion of the person holding the data and the state statute or federal law does not provide any standards which limit the exercise of such discretion. In such cases, the proper classification of the data is private.

3. A state agency rule, an executive order, and administrative decision, or a local ordinance shall not classify data as "confidential", or use wording to make data inaccessible to the data subject unless there is a state statute or federal law as the basis for the classification.

E. Private Data, as defined in § 15.162, subd. 5a of the Act, shall only include data which is expressly classified by either a state statute, including the provisions of § 15.1642 of the Act, or federal law.

1. Data is private if a state statute or federal law provides substantially that:

a. Certain data shall not be available to the public but shall be available to the subject of that data;

b. Certain data shall not be available to anyone, except the data subject or his designated representative such as an attorney;

c. Certain data shall be confidential and the person the data is about may view the data at reasonable times; or

d. Certain data shall be confidential and may be shown to the data subject at the discretion of the person holding the data. Such data shall be private if the state statute or federal law does not provide standards which limit the exercise of the discretion of the person maintaining the data.

2. Data is not private if:

a. A federal agency rule provides substantially that as a part of its plan for implementation of a certain federal

program, a state agency, statewide system, or political subdivision must provide for the confidentiality of data obtained from program subjects.

3. A state agency rule, an executive order, an administrative decision or a local ordinance shall not classify data as "private", or use wording to make data inaccessible to the public unless there is a state statute or federal law as the basis for the classification.

F. Public Data shall mean "data on individuals", as defined in § 15.162, subd. 5b of the Act, which is neither private nor confidential data~~;~~. ~~and-which-is-data-that-is-an-official-record pursuant-to-Minn.-Stat.-§-15.17.~~

~~1. Data-is-public-if:~~

~~a. A-state-statute-or-federal-law-substantially provides-that-certain-data-shall-be-made-available-to-the-public, pursuant-to-Minn.-Stat.-§-15.17,-or-any-other-similar-wording.~~

~~b. A-state-statute-or-federal-law-substantially requires-the-collection-of-certain-data-by-a-state-agency, political-subdivision-or-statewide-system,-and-does-not-classify that-data-as-private-or-confidential.~~

~~c. A-state-agency,-statewide-system,-or-political subdivision,-without-any-express-enabling-authority-to-do-so,~~

~~collects certain data because that data is necessary to its operations, as defined at 2 MCAR § 1.216, B.1.~~

1. This rule shall not limit the ability of an entity to apply for temporary classifications of data pursuant to § 15.1642 of the Act.

G. Designee ~~means any person designated by a responsible authority to be in charge of individual file(s) or system(s) containing "data on individuals"~~ shall have the meaning given that term by Section Four, Chapter 328, Minnesota Session Laws, 1979.

H. Entity means any governmental agency subject to the requirements of the Act, including state agencies, political subdivisions, and statewide systems as those terms are defined in § 15.162 of the Act.

1. State agency shall include any entity which is given power of statewide impact by statute or executive order.

2. Political subdivision shall include those local government entities which are given powers of less than statewide impact by statute or executive order.

3. Statewide systems shall include, but are not limited to, record keeping and data administering systems established by statute, federal law, administrative decision or agreement, or joint powers agreement.

a. Statewide systems shall include, but are not limited to, the Criminal Justice Information System administered by the Bureau of Criminal Apprehension, the Statewide Accounting System, ~~the Minnesota Education Computing Consortium;~~ and the various welfare systems primarily administered by the Department of Public Welfare.

I. Federal Law means United States Code, rules and regulations of federal agencies as published in the ~~Federal Register~~ Code of Federal Regulations, and federal case law, including decisions of any court in the federal judicial system.

J. Individual means any living human being. Individual shall not include any fictional entity or business such as a corporation, association, partnership, or sole proprietorship even in those instances where the name of such an entity or business includes the name of a natural person.

K. Records Management Act means Minn. Stat. § 138.17.

L. Responsible Authority means the individual in each entity who is designated or appointed pursuant to § 15.162, subd. 6 of the Act.

1. In state agencies, the Responsible Authority shall be as follows, unless otherwise provided by state law:

a. Departments: the commissioner of the department.

b. Constitutional Offices: the constitutional officer.

c. University of Minnesota: the individual appointed by the Board of Regents.

d. All other state agencies: the chief executive officer, or if none, then an individual chosen by the agency's governing body.

2. In political subdivisions, the Responsible Authority shall be as follows, unless otherwise provided by state law:

a. Counties: each elected official of the county shall be the Responsible Authority for his respective office. An individual who is an employee of the county shall be appointed by the county board to be the Responsible Authority for any data administered outside the offices of elected officials.

b. Cities: the city council shall appoint an individual who is an employee of the city.

c. School Districts: the school board shall appoint an individual who is an employee of the school district.

d. Nonprofit Corporations or Nonprofit Social Service Agencies: unless a statute or the governmental entity which created the corporation or agency appoints an individual,

the governing body of the corporation or agency shall appoint an individual. If no appointment is made, the chief executive officer of the nonprofit corporation or agency shall be the Responsible Authority. If the corporation or agency is part of a statewide system, the Responsible Authority for the statewide system shall be the Responsible Authority for the corporation or agency as determined by this rule.

e. All other political subdivisions: the governing body shall appoint an individual who is an employee of the political subdivision.

3. In "Statewide Systems", the Responsible Authority shall be as follows, unless otherwise provided by state law:

a. The commissioner of any state department or any executive officer designated by statute or executive order as responsible for such a system; or

b. If a state statute or executive order does not designate an individual as Responsible Authority, the Commissioner of Administration shall appoint the Responsible Authority after the entities which participate in the system jointly apply for such an appointment in a form provided by the Commissioner of Administration.

M. Summary Data, as defined in § 15.162, subd. 9 of the Act, means data which has been extracted, manipulated, or summarized

from private or confidential data, and from which all data elements that could link the data to a specific individual have been removed.

1. Summary data includes, but is not limited to, statistical data, case studies, reports of incidents, and research reports.

2. Once it is summarized from private or confidential data, summary data remains ~~Data is~~ summary ~~data~~ if the Responsible Authority maintains any list of numbers or other data which could uniquely identify any individual in the summary data ~~is~~ physically separated from the summary data and the Responsible Authority does ~~is~~ not ~~made~~ make such list available to persons who gain access to, or possession of the summary data.

2 MCAR § 1.203. Access to Public Data. The Responsible Authority shall comply with the following general rules governing access to public data.

A. The Responsible Authority shall provide access to public data to any person, regardless of that person's interest in the data.

1. The Responsible Authority shall establish procedures to describe how such access may be gained.

a. In such procedures, the Responsible Authority may limit the time during which ~~that public~~ access to public data is available to the time during which the normal operations ~~office hours~~ of the agency are conducted.

b. In such procedures, the Responsible Authority shall provide for a response to a request for access within a reasonable time.

c. The Responsible Authority ~~shall~~ may charge a reasonable fee for providing copies of public data~~;-unless-the costs-incurred-by-the-entity-in-providing-the-copies-are-minimal~~.

d. In determining the amount of the reasonable fee, the Responsible Authority shall be guided by the following:

(1) The cost of materials, including paper, used to provide the copies.

(2) The cost of the labor required to prepare the copies.

(3) Any schedule of standard copying charges as established by the agency in its normal course of operations.

(4) Any special costs necessary to produce such copies from machine based record keeping systems, including but not limited to computers and microfilm systems.

(5) Mailing costs.

2 MCAR § 1.204. Access to Private Data. Pursuant to §§ ~~15.1641~~ 15.163 and 15.162, subd. 5a of the Act, the Responsible Authority shall comply with the following rules concerning access to private data:

A. Access to private data shall be available only to the following:

1. The subject of such data~~.~~, as limited by any applicable statute or federal law.

2. Individuals within the entity, whose work assignments reasonably require access.

3. Entities and agencies as determined by the Responsible Authority who are authorized by statute, including ~~§ 15.1641 (e)~~ 15.163, subd. 4 of the Act, or federal law to gain access to that specific data.

4. Entities or individuals given access by the express written direction of the data subject.

B. The Responsible Authority shall establish written procedures to assure that access is gained only by those parties identified in Part A of this rule.

1. In those procedures, the Responsible Authority shall provide for reasonable measures ~~that will~~ to assure that the person seeking to gain access to the private data is actually the subject of that data or the authorized representative of the data subject.

2. Examples of such reasonable measures include, but are not limited to, the following:

a. Requiring the person seeking to gain access to appear at the offices of the entity to gain such access or, in lieu of a personal appearance, requiring the ~~notarized~~ signature of any data subject who is unable to appear at the offices of the entity.

b. Requiring the person to provide reasonable identification.

C. The Responsible Authority may limit the time that access is available to the data subject to the normal working hours of the agency.

D. The Responsible Authority shall not charge the data subject any fee in those instances where the data subject only desires to view private data.

E. The Responsible Authority shall charge the data subject a reasonable fee for providing copies of private data.

1. In determining the amount of the reasonable fee, the Responsible Authority shall be guided by the criteria set out in 2 MCAR § 1.203 concerning access to public data.

2 MCAR § 1.205 Access to Private Data Concerning Data Subjects Who are Minors. Pursuant to §§ ~~15.1641,-and~~ 15.162, subd. 4 and subd. 5a and 15.163 of the Act, the Responsible Authority shall comply with the following rules concerning access:

A. In addition to the particular requirements of this rule, access to private data concerning a minor data subject shall be subject to the requirements of 2 MCAR § 1.204 concerning access to all private data.

B. Access to private data concerning minors shall be available only to the following:

1. Those parties identified as having access to private data under ~~part~~ Section A of 2 MCAR § 1.204.

2. Subject to the provisions of Minn. Stat. § 15.162, subd. 4, any other applicable statute, and the exception set out at ~~part G-1~~ 1.205, C. 1. below, the parents of the minor data subject.

a. For purposes of this rule, the Responsible Authority shall presume the parent has the authority to exercise the rights inherent in the Act unless the Responsible Authority has been provided with evidence that there is a state law or court order governing such matters as divorce, separation, or custody, or a legally binding instrument which provides to the contrary.

C. Pursuant to the provisions of Minn. Stat. § 15.162, subd. 4, the Responsible Authority shall establish procedures to provide access by the parents of a minor data subject to private data concerning that minor, subject to the following:

1. The Responsible Authority may deny parental access to private data when the minor, who is the subject of that data, requests that the Responsible Authority deny such access.

a. The Responsible Authority shall provide minors from whom the entity collects private, or confidential data with a notification that the minor individual has the right to request that parental access to private data be denied.

ab. The Responsible Authority may require the minor data subject to submit a written request that the data be withheld. The written request shall set forth the reasons for denying parental access and shall be signed by the minor.

2. Upon receipt of such a request, the Responsible Authority shall determine if honoring the request to deny parental access would be in the best interest of the minor data subject.

a. In making the determination, the Responsible Authority shall be guided by at least the following:

(1) Whether the minor is of sufficient age and maturity to be able to explain the reasons for and to understand the consequences of the request to deny access.

(2) Whether the personal situation of the minor is such that denying parental access may protect the minor data subject from physical or emotional harm.

(3) Whether there is ground for believing that the minor data subject's reasons for precluding parental access are reasonably accurate.

(4) Whether the data in question is of such a nature that disclosure of it to the parent could lead to physical or emotional harm to the minor data subject.

~~(5) Whether the data in question is subject to the right of parental access outlined in the "Family Educational Rights and Privacy Act of 1974", Public Law 93-380, and the rules promulgated thereunder.~~

~~(6)~~ (5) Whether the data concerns medical, dental or other health services provided pursuant to Minn. Stat. §§ 144.341 through 144.347. If so, the data may be released only if failure to inform the parent would seriously jeopardize the health of the minor.

3. The Responsible Authority shall not deny access by parents to data that is considered an "education record", as that term is defined in Title 45 Code of Federal Regulations, Part 99, Section 99.3, unless the minor is enrolled as a full time student in a post-secondary educational institution.

2 MCAR § 1.206. Access to Confidential Data. Pursuant to Minn. Stat. §§ ~~15.1641~~ 15.163 and 15.162, subd. 2a, the Responsible Authority shall comply with the following rules concerning access to confidential data:

A. Access to confidential data is available only to the following:

1. Individuals within the entity, whose work assignments reasonably require access.

2. Entities and agencies who are authorized by statute, including § 15.1641~~4~~3 of the Act, or federal law to gain access to that specific data.

B. The Responsible Authority shall establish written procedures to assure that access may be gained only by those parties identified in Part A of this rule.

1. In the drafting and administration of those procedures, the Responsible Authority shall provide measures by which data subjects shall be informed, upon request, if they are the subjects of confidential data.

a. The Responsible Authority shall not disclose the actual confidential data to the data subjects, but shall inform them whether confidential data concerning them is or is not retained.

b. The Responsible Authority shall take reasonable measures to assure that the person making inquiry is actually the individual data subject~~.~~ or the authorized representative of the data subject.

c. Reasonable measures ~~may~~ include, but are not limited to:

(1) Requiring the inquiring person to appear at the office of the entity to make his/her request.

(2) Requiring the inquiring person to provide identification.

(3) Requiring the notarized signature of any data subject who is unable to appear at the offices of the entity.

2 MCAR § 1.207. Access to Arrest Information. Pursuant to § 15.162, subd. 1a, 2a, and 5a of the Act, the Responsible Authority, shall comply with the following rules concerning access to arrest information:

A. For the duration of time, defined in Part B of this rule, that immediately follows the creation of data constituting arrest information, the Responsible Authority shall make such information available to anyone who requests it in writing, by personal appearance, by telephone inquiry, or any other means.

B. For purposes of this rule, "duration of time" commences with the creation or recording of the arrest information subsequent to the actual detention or citation of the arrested party. "Duration of time" ends at that point in time when an arrested party is:

1. Either released without a criminal complaint being filed against him/her; or

~~2.--Appears-before-a-judicial-officer-for-the-offense for-which-he/she-was-arrested,-or-any-lesser-included-offense-as described-in-the-Rules-of-Criminal-Procedure-as-adopted-by-the Minnesota-Supreme-Court.~~

2. Is released from the supervision of any component of the criminal justice system.

C. During the duration of time described in Part B of this rule, the Responsible Authority shall not be limited to publicly releasing only arrest information, as defined by § 15.162, subd. 1a of the Act. The Responsible Authority may release additional information after consideration of at least the following:

1. Whether the status afforded to certain data is investigative data, pursuant to § 15.162, subd. 2a of the Act, is no longer needed to protect the integrity of an investigation.

2. Whether there is concern and interest on the part of the public in the person arrested or the alleged crime committed.

3. Whether the release of additional data and its subsequent publication may prejudice the arrested individual's right to a fair and impartial trial.

4. Whether the data subject has requested that arrest disposition data pertaining to that data subject be disseminated.

5. Whether the identity of any victims of or witnesses to the crime should be protected.

D. The Responsible Authority shall not make available to the public any individually identifiable data concerning the detention of a juvenile individual, unless that juvenile is judicially certified to be tried as an adult as described in the Minnesota Rule of Criminal Procedure. The Responsible Authority shall make any data concerning the detention of a juvenile available to the parents of the juvenile.

2 MCAR § 1.208. Access to Investigative Data. Pursuant to Minn. Stat. §§ 15.162, subd. 2a and 15.1641 of the Act, the Responsible Authority shall comply with the following general rules concerning access to investigative data:

A. Investigative data is confidential data, pursuant to § 15.162, subd. 2a(b). The Responsible Authority shall comply with the provisions of 2 MCAR § 1.206, concerning access to confidential data.

B. The Responsible Authority shall determine that data maintained by his entity is investigative data only if all criteria set out in Parts 1, 2, and 3 of this section are met.

1. Collecting Agency Criteria. The data is collected, created or maintained by or at the direction of one of the following entities, or by an agent of such entity:

a. Law Enforcement agencies, whose agents are given arrest powers, including, but not limited to those entites listed in 2 MCAR $ ~~1.201~~ 1.202, B.1.

~~b.--Public-Attorneys,-who-are-given-the-statutory or-constitutional-authority-to-prosecute-or-to-defend-civil-or criminal-actions-as-defined-by-the-Minnesota-Rules-of-Civil Procedure-and-the-Minnesota-Rules-of-Criminal-Procedure-including, but-not-limited-to,-municipal-and-county-prosecutors-and-members of-the-Attorney-General's-staff.~~

eb. Judicial entities, whose agents are given the statutory or constitutional authority to adjudicate cases and to render sentences.

dc. Any agency given statutory authority to revoke or suspend licensure.

ed. Any entity which has a reasonable expectation that certain data, in its possession may become the subject of a legal action, as set forth in Part 2 of this section.

2. Purpose of Collection Criteria. The data is collected or created for the purpose of the commencement of a legal action. Any of the following shall constitute a "legal action", for the purposes of this rule, and as used in Minn. Stat. § 15.162, subd. 2a(b):

a. Arrest of any individual.

b. Issuance of a citation, complaint, or an indictment as described in Minnesota Rules of Criminal Procedure.

c. Service of a civil complaint on behalf of the state, a state agency, or a political subdivision.

d. Service of a civil answer on behalf of the state, a state agency, or a political subdivision.

e. Maintaining or prosecuting a civil or criminal action on behalf of the state, a state agency, or political subdivision.

f. Conducting any arbitration proceeding pursuant to Chapter 572 of Minnesota Statutes.

g. Conducting any proceeding which may lead to the suspension or revocation of any type of license issued by a state agency or political subdivision.

3. Active Data Criteria. Active data includes:

a. Data collected for the purpose of the commencement of a criminal action in which all perpetrators of the criminal violation have not been apprehended, the matter has not been fully adjudicated, the statute of limitations for the

alleged violation has not run, or all rights of appeal in the judicial system have not been exhausted.

b. Data collected for the purpose of bringing or defending a civil action where that action has not been finally resolved, including exhaustion or extinguishment of all rights of appeal in the judicial system.

c. Data collected for the purpose of participation in an arbitration proceeding where that proceeding has not resulted in a binding decision, including exhaustion of all rights of appeal in the judicial system.

d. Data collected for the purpose of participation in a license revocation or suspension proceeding where that proceeding has not resulted in a binding decision, including exhaustion of all rights of appeal in the judicial system.

2 MCAR § 1.209. Access to Summary Data. Pursuant to Minn. Stat. § ~~15.1641-(d)~~ 15.163, subd. 7, the Responsible Authority shall comply with the following general rules concerning access to summary data:

A. Summary data is public data~~.~~, unless classified by statute, federal law or temporary classification as non-public. The Responsible Authority shall comply with 2 MCAR § 1.203, concerning access to public data.

B. The Responsible Authority shall prepare and implement procedures in his/her agency to assure that access to summary data is given to anyone who requests such data. In the preparation and administration of such procedures, the Responsible Authority shall comply with the following:

1. Preparation of summary data may be requested by any person. The request shall be in writing in a form provided by the Responsible Authority. Within ten days of the receipt of such a request, the Responsible Authority shall inform the requestor of the estimated costs if any, pursuant to subd. 2 of this rule and subject to the provisions of that section either:

a. Provide the summary data requested; or

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

c. Provide access to the requestor to the private or confidential data for the purpose of the requestor's preparation of summary data, pursuant to § ~~15.1641-(d)~~ 15.163, subd. 7, of the Act and subd. 4 of this section~~.~~; or

d. Provide a written statement to the requestor stating reasons why the Responsible Authority has determined that the requestor's access would compromise the private or confidential data.

2. Any costs incurred in the preparation of summary data shall be borne by the requesting person. In assessing the costs associated with the preparation of summary data, the Responsible Authority shall:

a. Be guided by the provisions of 2 MCAR § 1.203 in determing costs.

b. Provide to the requesting person an estimate of the costs associated with the preparation of the summary data.

c. Prior to preparing or supplying the summary data, collect any funds necessary to reimburse the entity for its costs.

d. Charge no more than reasonable copying costs when the summary data being requested requires only copying and no other preparation.

e. Take into account the reasonable value to the entity of the summary data prepared.

3. For the purposes of administering Minn. Stat. § ~~15.1641-(d)~~ 15.163, subd. 7, the following terms shall have the meanings given them.

a. "Administrative officer" includes, but is not limited to, the entity's research director, statistician, or computer center director.

b. "Person outside" the entity includes the person requesting the summary data or any other person designated by the person requesting the data.

4. A non-disclosure agreement, as required by § ~~15.1641-(d)~~ 15.163, subd. 7 of the Act shall contain at least the following:

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

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

c. A statement that the preparer understands he/she may be subject to the civil or criminal penalty provisions of the Act in the event that the private or confidential data is disclosed.

5. Methods of preparing summary data include but are not limited to the following:

a. Removing from a set of data, a file, or a record keeping system all unique personal identifiers so that the data that remains fulfills the definition of summary data as defined by § 15.162, subd. 9 of the Act.

b. Removing from the entity's report of any incident, or from any collection of data similar to an incident report, all unique personal identifiers so that the resulting report fulfills the definition of summary data in § 15.162, subd. 9 of the Act.

c. For the purpose of this rule, "removing all unique personal identifiers" includes but is not limited to:

(1) Blacking out personal identifiers on paper records.

(2) Tearing off or cutting out the portions of paper records that contain the personal identifiers.

(3) Programming computers in such a way that printed ~~or~~, terminal or other forms of output does not contain personal identifiers.

2 MCAR § 1.210. Classification of Data. In order to comply with the provisions of §§ 15.162, ~~15.1641,~~ 15.165 and 15.163 of the Act the Responsible Authority shall:

A. Review and identify all of the types of data maintained by the entity, including data retained as active and inactive.

B. ~~Determine the private, confidential, or public classification for easy type of data;~~ Determine what types of data maintained by the entity are classified as private or confidential, according

to the definitions of those terms pursuant to § 15.162 of the Act and 2 MCAR § 1.202.

C. Identify either a state statute or provisions of federal law supporting any determination that certain data is either private or confidential.

D. Administer all agency data in accordance with the determinations made under 2 MCAR § 1.210 B.

2 MCAR § 1.211. Authority of the Responsible Authority. ~~Jurisdiction, as that term is used in § 15.1641 (a) of the Act, means that the Responsible Authority shall have the authority to:~~ Pursuant to § 15.162 through 15.1642 of the Act, the Responsible Authority shall have the authority to:

A. Implement the Act and these rules in each entity.

B. Make good faith attempts to resolve all administrative controversies arising from the entity's practices of creation, collection, use, and dissemination of data.

C. Prescribe changes to the administration of the entity's programs, procedures, and design of forms to bring those activities into compliance with the Act and with these rules.

D. Take all administrative actions necessary to comply with the general requirements of the Act, particularly Minn. Stat. § 15.165, and these rules.

E. Where necessary, direct designees to perform the detailed requirements of the Act and these rules under the general supervision of the Responsible Authority.

2 MCAR § 1.212. Appointment of the Responsible Authority.

A. Pursuant to § 15.162, subd. 6 of the Act, the governing body of each political subdivision and the governing body of each state agency whose activities are subject to the direction of a governing body shall, within 30 days of the effective date of these rules, if it has not done so, appoint a Responsible Authority.

1. This rule shall not affect the appointments of Responsible Authorities made previous to the adoption of this rule.

2. The governing body shall confer on the Responsible Authority full administrative authority to carry out the duties assigned by the Act and by these rules.

3. Governing bodies may use the forms set forth in the appendix to these rules to appoint the Responsible Authority.

2 MCAR § 1.213. Appointment Power of the Responsible Authority. Pursuant to § ~~15.1641-(a)~~ 15.1621, subd. 2 of the Act, the

Responsible Authority shall, if he deems it to be in the best interest of the administration and enforcement of the Act, appoint designees who shall be members of the staff of the entity. In the exercise of this appointment power, the Responsible Authority shall comply with the following:

A. The appointment order shall be in writing and copies of the order constitute public data on individuals, pursuant to Minn. Stat. § 15.162, subd. 5(b) of the Act.

B. The Responsible Authority shall instruct any designees in the requirements of the Act and of these rules. If the Responsible Authority deems it necessary, such instruction shall include:

1. Distribution to designees of written materials describing the requirements of the Act and of these rules.

2. Preparation of training programs whose objective is to familiarize agency personnel with the requirements of the Act and of these rules.

3. Requiring attendance of designees and other entity personnel at training programs held within or outside the entity.

2 MCAR § 1.214. Duties of the Responsible Authority Relating to Public Accountability. Pursuant to § 15.163 of the Act, the

duties of the Responsible Authority shall include, but not be limited to the following:

A. For the purposes of public accountability, the Responsible Authority shall, within sixty days of the effective date of these rules, or until August 1 of each year when the requirements of Part B of this rule are fully complied with, place his/her name, job title and business address, and the name(s) and job titles of any designees selected by the Responsible Authority on a document.

1. Such document shall be made available to the public and/or posted in a conspicuous place by each entity.

2. The document shall identify the Responsible Authority or designees as the persons responsible for answering inquiries from the public concerning the provisions of the Act or of these rules.

B. In the public document to be prepared or updated by August 1 of each year as required by § 15.163 of the Act, the Responsible Authority shall identify and describe by type all records, files, or processes maintained by his/her entity which contain private or confidential data.

1. In addition to the items to be placed in the public document as required by § 15.163 of the Act, the Responsible Authority shall include the following:

a. The name, title, and address of designees appointed by the Responsible Authority.

b. Identification of the files or systems for which each designee is responsible.

c. A citation of the state statute or federal law which classifies ~~the~~ each type of data as private or confidential.

2. The Responsible Authority shall draft the descriptions of the types of records, files, and processes in easily understandable English. Technical or uncommon expressions, understandable only by a minority of the general public shall be avoided, except where required by the subject matter.

3. The Responsible Authority may use the form set forth in the appendix to these rules to prepare this public document.

2 MCAR § 1.215. Duties of the Responsible Authority Relating to the Administration of Private and Confidential Data. In order to administer the requirements of § ~~15.1641-(e)~~ 15.163, subd. 4(a) of the Act, the Responsible Authority shall determine for each type of record, file, or process identified in 2 MCAR § 1.214 whether the data contained therein was collected prior or subsequent to August 1, 1975.

A. For each type of record, file, or process containing data collected prior to August 1, 1975, the Responsible Authority shall:

1. Review the federal, state or local legal enabling authority which mandated or necessitated the collection of the private or confidential data.

2. Based on that review, determine the lawful purpose for the collection of the data at the time it was originally collected.

3. Direct the staff of the entity that private or confidential data collected prior to August 1, 1975, shall not be used, stored, or disseminated for any purpose, unless that purpose is authorized by the enabling authority which was in effect at the time the data was originally collected.

B. For each type of record, file, or process containing private or confidential data collected on or subsequent to August 1, 1975, the Responsible Authority shall:

1. Review the legal enabling authority which mandates or necessitates the collection of the data.

2. Identify the purposes for the collection of and the intended uses of all private or confidential data that have been communicated to data subjects or should have been communicated to data subjects at the time of data collection, pursuant to § 15.165, subd. 2 of the Act.

C. Using the purposes and uses identified in Parts A and B of this rule, the Responsible Authority shall:

1. Prepare lists which identify the uses of and purposes for the collection of private or confidential data for each type of record, file or process identified in 2 MCAR § 1.214.

a. Each list shall identify all persons, agencies, or entities authorized by state or federal law to receive any data disseminated from the particular record, file or process.

2. Pursuant to § 15.165, subd. 2 of the Act, either:

a. Attach each list identifying purposes, uses and recipients of data to all agency forms which collect the private or confidential data that will be retained in each record, file or process; or

b. Communicate, in any reasonable fashion, the contents of each list to data subjects at the time particular data that will be retained in each record, file, or process is collected from them. For purposes of this section, "reasonable fashion" shall include, but not be limited to:

(1) Oral communications made to data subjects.

(2) Providing data subjects with brochures that describe the entity's purposes for the collection of and the

uses to be made of private and confidential data.

D. In administering the entity's private or confidential data consistent with the provisions of the rules, the Responsible Authority shall:

1. Educate entity personnel as to authorized purposes and uses.

2. Prepare administrative procedures that will acquaint entity pesonnel with authorized purposes and uses.

3. Distribute policy directives requiring compliance with the entity's determination of authorized purposes and uses.

E. The Responsible Authority shall authorize a new purpose for the collection of private or confidential data or a new use for private or confidential data under any one of the following conditions:

1. If subsequent passage of federal or state legislation requires initiation of a new or different purpose or use pursuant to § ~~15.1641-(e)-(2),-of-the-Act,~~ 15.163, subd. 4(b), of the Act, or

2. The Responsible Authority, prior to initiation of the new or different purpose or use, complies with the provisions of either § ~~15.1641,-(e)-(1)-or-(3)~~ 15.163, subd. 4(a), subd. 4(c) or subd. 4(d) of the Act.

a. For the purposes of administration of Minn. Stat. § ~~15.1641-(e)-(1)~~ 15.163, subd. 4(a) or subd. 4(c), the Responsible Authority shall file a statement on a form provided by the Commissioner.

A Responsible Authority shall not initiate a new or different purpose or use of private or confidential data until the Responsible Authority receives written approval from the Commissioner.

b. For the purposes of Minn. Stat. § ~~15.1641-(e)-(3)~~ 15.163, subd. 4(d) the following term shall have the meaning given it:

(1) "Informed consent" means the data subject possesses and exercises sufficient mental capacity to make a decision which reflects an appreciation of the consequences of allowing the entity to initiate a new purpose or use of the data in question.

c. For the purposes of the administration of Minn. Stat § ~~15.1641-(e)-(3)~~ 15.163, subd. 4(d), the Responsible Authority shall comply with the following:

(1) The Responsible Authority shall not take any action to coerce any data subject to give an "informed consent". The Responsible Authority shall explain the necessity for or consequences of the new or different purpose or use.

(2) All informed consents shall be given in writing. Prior to any signature being affixed to it by the data subject, such writing shall identify the consequences of the giving of informed consent.

(3) If the Responsible Authority makes reasonable efforts to obtain the informed consent of a data subject and if those efforts are not acknowledged in any way, the Responsible Authority shall interpret the silence of the data subject as the giving of an implied consent to the new or different purpose or use of the data.

(a) For purposes of this section, "reasonable efforts" shall include:

(i) Depositing in the United States Mail, postage pre-paid and directed to the last known address of the data subject, at least two communications requesting informed consent.

(ii) Waiting for a period of not less than 60 days for a response to the second request.

(4) The data subject may give informed consent to less than all of the data elements in any list of data elements presented by a Responsible Authority, thereby giving only partial consent.

(a) Only those elements that the data subject has expressly consented to shall become part of the new or different purpose or use.

D. If the Responsible Authority seeks an individual's informed consent to the release of private data to an insurer or the authorized representative of an insurer, the Responsible Authority shall comply with the provisions of Minn. Stat. § 15.163, subd. 4 (d), (1) through (7).

2 MCAR § 1.216. Duties of the Responsible Authority as They Relate to the Administration of all Entity Data. Pursuant to § ~~15.1641-(b)~~ 15.163, subd. 3 of the Act, the Responsible Authority shall, within eighteen months of the effective date of these rules, formulate a plan that will provide for the review and analysis of the data administration practices of the entity.

A. In the formulation of this plan, the Responsible Authority shall at least provide for the preparation of a list of or index to all data or types of data currently collected, stored, used, or disseminated by the entity.

1. The list or index developed shall include the identification of the state statute(s), federal law(s), or local ordinance(s) that authorize(s) the programs or functions for which data or types of data are ~~is~~ collected, or which authorize(s) the actual ~~data~~ collection, storage, use or dissemination of data or types of data.

a. The plan shall further provide for the list or index to be updated when new or different data collection, storage, use or dissemination is authorized.

b. This list or index shall be available to members of the general public, upon request.

B. The Responsible Authority shall use this plan and the list or index developed to aid in the determination of whether collection and storage of data and use and dissemination of private or confidential data is necessary.

1. For purposes of this section, data is necessary if:

a. The particular data is both:

(1) Required to carry out programs and functions that are expressly or impliedly authorized by a provision of state statute, federal law or a local ordinance; and

(2) Periodically examined, updated, modified or referred to by the entity; or

b. The entity would be unable to fulfill its duties without undue or increased burden or expense, if the particular data were not collected, stored, used or disseminated; or

c. Retention of the particular data is required in the event that a legal action is brought against or by the entity; or

d. Retention of the particular data is essential to comply with a state or federal requirement that data be retained for a specified period for the purposes of auditing, records retention, historical interest, and other similar purposes.

C. For any data determined to be not necessary pursuant to Part B of this rule, the Responsible Authority shall provide for the following activities in the entity's plan.

1. Taking all actions ~~which include making changes to forms designs, rewriting procedures, and so forth,~~ , including modification of the entity's data collection forms and data collection procedures, to assure that all ~~such~~ unnecessary data is no longer collected and stored and all ~~such~~ private and confidential data determined to be not necessary is no longer used and disseminated. Private data shall continue to be disseminated upon request by the data subject.

2. Disposing of ~~such~~ data determined to be not necessary pursuant to the procedures of the Records Management Act.

a. Inquiries concerning procedures for disposition of data may be directed to the Records Management Division, Department of Administration, St. Paul, Minnesota, 55155.

D. In the formulation of the plan described in Part A of this rule, the Responsible Authority shall provide for the establishment of administrative mechanisms and procedures that comply with § ~~15.1641(e)~~ 15.163, subd. 5 of the Act. For purposes of this section,

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

2. "Complete" means that the data in question reasonably reflects the history of an individual's transactions with the particular entity. Omissions in an individual's history that place the individual in a false light shall not be permitted.

3. "Current" means that the data in question must be logically related to the entity's required and actual use of the data in its day-to-day operations.

2-MCAR-§-1.217--Duties-of-the-Responsible-Authority-as-They-Relate to-Computerized-Data.--For-the-purposes-of-the-administration-of §-15.1641-(e)-of-the-Act,-the-Responsible-Authority-shall-be guided-by-the-following:

A.--"Directly-Accessible-Files"-means-files-maintained-by any-entity-which-contain-private-or-confidential-data,-to-which access-can-be-made-or-updating-performed-through-the-use-of-any type-of-communication-terminal,-including,-but-not-limited-to, teletypewriters-and-cathode-ray-tube-terminals.

B.--Within-180-days-of-the-effective-date-of-these-rules,-the Responsible-Authority-shall-perform-an-audit-of-the-physical-and software-security-measures-that-the-entity-has-installed-to protect-the-integrity-of-"directly-accessible-files".

C.--The-nature-and-extent-of-the-audit-shall-be-at-the-discretion-of-the-Responsible-Authority,-subject-to-the-following:

1.--The audit shall emphasize a review of any measures taken to assure that private or confidential data is not accessible to the public through the use of a communications terminal.

2.--The audit shall include a review of the measures taken to assure all of the entity's computer based data is protected from tampering by unauthorized persons.

D.--If it reasonably appears to the Responsible Authority that there are weaknesses in the entity's data security procedures, the Responsible Authority shall:

1.--Provide for terminal security and system and data integrity through the establishment of appropriate security measures.

a.--Appropriate security measures include, but are not limited to, usage of password systems, establishment of procedures to assure physical security of terminals, utilization of system usage audits, and update verification routines, and establishments of limits on the system usage capabilities given to terminals.

E.--Auditing security measures on an annual basis shall be a part of the ongoing administration of the entity's computerized data system.

2 MCAR § ~~1.218~~ 1.217 Administrative Appeal, Pursuant to § 15.165, subd. 4 of the Act, an individual may appeal an adverse determination of a Responsible Authority to the Commissioner of Administration.

A. The appeal shall follow the procedures established in Minnesota Statutes, Chapter 15, as amended, and the rules of the Office of Hearing Examiners relating to Contested Case Proceedings.

B. Notice of an appeal must be submitted to the Commissioner within a reasonable time of the determination made by the Responsible Authority pursuant to § 15.164, subd. 4 of the Act.

1. The notice shall be in writing and addressed to the Commissioner of Administration, State of Minnesota, 50 Sherburne Avenue, St. Paul, Minnesota 55155.

2. The notice shall contain the following information:

a. The name, address, and phone number, if any, of the appealing party.

b. The name of the Responsible Authority and the entity which he or she represents.

c. A description of the nature of the dispute, including a description of the data.

d. A description of the desired result of the appeal.

3. The Commissioner may require additional information if it is reasonably necessary in order to establish the Contested Case Proceeding.

4. Upon written request of the data subject stating reasons, the appeal may be processed under the name of a pseudonym.

C. After a preliminary review of the notice and any supporting documentation, the Commissioner may upon written notice to all parties dismiss any sham, capricious or frivolous appeal or any appeal not within the jurisdiction of the Department.

~~C~~D. The Department of Administration shall be reimbursed for all costs associated with the Contested Case Proceeding by the entity whose Responsible Authority has been the impetus for the individual's appeal to the Commissioner.

1. The Commissioner shall establish appropriate accounting procedures to provide to the entity an itemized invoice.

2 MCAR § 1.219 General Powers of the Commissioner. Pursuant to § 15.163, subd. 2 of the Act and to assist in the general implementation and enforcement of the Act, the Commissioner shall have the following powers:

A. If the Commissioner determines that certain information is relevant to monitoring any entity's data collection and handling

practices, policies and procedures, the Commissioner shall require the Responsible Authority of such entity to submit the information.

B. Any inquiries concerning the Act or these rules and any information submissions required to be made by Section A of this rule shall be directed to the Data Privacy ~~Unit~~ Division, Department of Administration, State of Minnesota, 50 Sherburne Avenue, St. Paul, Minnesota 55155.

C. The Data Privacy ~~Unit~~ Division shall respond promptly to all inquiries within personnel and budgetary limitations.

2 MCAR § 1.220. Duties of the Commissioner Relating to Temporary Classification of Data. Pursuant to Minn. Stat. § 15.1642, the Commissioner and Responsible Authorities shall comply with the following:

A. The Responsible Authority, pursuant to § 15.162, subd. 6 of the Act, shall prepare any application for ~~emergency~~ temporary classification in writing in a form provided by the Commissioner. Copies of the form are available from the Data Privacy Division.

~~1.--The-form-for-an-application-is-set-out-in-the-appendix to-these-rules.--Copies-of-the-form-are-available-from-the-Data Privacy-Unit.~~

B. For the purposes of the administration of § 15.1642 of the Act, the following terms have the meanings given to them:

1. "Days" means calendar, not working days.

2. "Upon filing" means upon receipt of either an original or amended application by the Commissioner.

3. "Date of Disapproval" means the date the Responsible Authority actually receives the disapproval notification from the Commissioner.

4. "Within ~~20~~ 25 days of submission to the Attorney General" means within ~~20~~ 25 days of the date that the Attorney General's Office in the Department of Administration actually receives the record from the Commissioner.

C. Applications for ~~emergency~~ temporary classification of data shall be submitted to the Data Privacy ~~Unit~~ Division, Department of Administration, State of Minnesota, St. Paul, Minnesota 55155.

D. If the Data Privacy ~~Unit~~ Division requires the Responsible Authority to submit additional information in support of the application, that application is deemed to have been filed on the date the additional material is received by the Data Privacy ~~Unit~~ Division. The Commissioner shall return any application to the applicant if the additional information requested is not received within 30 days.

~~E.--The-provisions-of-this-rule-shall-terminate-and-cease to-have-force-and-effect-on-whichever-of-the-following-dates or-events-occurs-later:~~

~~1.--On-August-1,-1979,-or~~

~~2.--On-the-effective-date-of-a-statute-that-repeals-the Commissioner's-authority-to-rule-on-emergency-classification-of data,-pursuant-to-Minn.-Stat.-§-15.1642,-subd.-3.~~

2 MCAR § 1.221. Severable Provisions. If any provisions of these rules are found invalid for any reason, the remaining provisions shall remain valid.

RECEIVED
DEC 06 1973
ATTORNEY GENERAL
ADMINISTRATIVE AGENCIES

DELEGATION

Shroeder Nursing Cne, Inc v Mutual of Omaha Insurance Co., 26 AdL 2d 1088 (ED Wis, 1970)

Delegation by Sec of HEW to private organization to determine reas. costs reimbursable under Act was proper.

United States v Cincinnati Transit, Inc., 31 AdL 2d 378 (SD Ohio, 1972)

Rules promulgated by Office of Emergency Preparedness in connection with wage + price "freeze" were issued pursuant to a constitutional subdelegation of powers by the President to the agency since there were "intelligible standards" governing that delegation.

→ Note Chap 15.0412 - subd. 3 gives all agencies authority for procedural rules

Legislative intent

The intent of the legislature must be ascertained from the language of the entire act read in the light of the object evidently in view.

In re Cold Spring Granite Co. (1965) 271 Minn 460, 136 NW2d 782.

It may consider: legislative history, subject matter as a whole, purpose of legislation, events leading to passage + modifications to law during course. Serv. Co. v Comm of Taxation (1960) 257 Minn 92, 100 NW2d 678

Every law should be construed so as to give effect to all its provisions

Beltrami Cnty v Hennepin Cnty (1963) 264 Minn 406, 119 NW2d 25

When meaning of stat. is doubtful great weight is to be given by courts to construction placed upon it by the dept. charged with its administration

Knopp v Gutterman (1960) 258 Minn 133, 102 NW2d 689

Introduction
Documents

(1) Order for hearing

(2) Affidavit of Receipt of See of State's List

(3) Certificate of Delivery of Sec. of State's List

(4) Affidavit of Mailing ~~to~~ a Memorandum, Notice of Hearing and Proposed Rules to ~~State~~
(a) State Agencies
(b) Political Subdivisions
(c) Those on Sec of State's List
Others
as required by 15.0412 and 15.162, subd 5)

(5) Memorandum from Richard Brubacher, C of Admin to
(a) State Agencies
(b) Political Subd.
etc.

(6) State Register, Vol 3, Number 9, Sep 4, 1978
(a) on page 346 ~~thru~~
Notice of Hearing
(b) on page 347
Proposed rules

(c) Financial Impact Stmt req by 15.0412, sub 7

(7) Stment of Need & Reasonableness
(a) All persons have had opportunity to review
(i) ~~st~~ Notice referenced
(ii) Filed with H.E. for at least 25 days
(b) Don Gemberling Director of Data Privacy Unit with Dept of Admin.
Donald Magraw, Asst Com of Dept of Admin.
Have to answer questions and familiar w/ rules and agency's Statement of Need.

Also submitted

(8) Materials received after Notice of Intent to Solicit Outside Opinion
State Register, Vol 2, No 48
June 5, 1978 at 2167

(9) With Stmt of Need - Materials received after Notice of Hearing - Utley letter

(10) Names of Witnesses

(11) Affidavit of Review of the proposed rules by Intergovernmental Information Systems Advisory Council - pursuant to 15.1671

ERRATA

to the proposed adoption of permanent rules governing the enforcement and administration of the "Minnesota Data Privacy Act", as published in the State Register, September 4, 1978

Page 347:

Rule 2 MCAR § 1.201, Subsection A, should read: "A. These rules shall apply to those governmental entities as defined by Minn. Stat. § 15.162, ..."

Pages 348-349:

Rule 2 MCAR § 1.202, Subsection E. following l.c., the Rule should read:

2. Data is not private if:

   a. A federal agency rule provides substantially that as a part of its plan for implementation of a certain federal program, a state agency, statewide system, or a political subdivision must provide for the confidentiality of data obtained from program subjects.

3. A state agency rule, an executive order, an administrative decision, or a local ordinance shall not classify data as "private", or use wording to make data inaccessible to the public unless there is a state statute or federal law as the basis for the classification.

Page 350:

In Rule 2 MCAR § 1.202, Section L. 3., paragraph a. should read:

   a. The commissioner of any state department or any executive officer designated by statute or executive order as responsible for such a system; or

Page 353:

In the introductory paragraph of 2 MCAR § 1.208, change the second to the last word in that paragraph from investigatory to investigative.

In 2 MCAR § 1.208, Section A. change the first word of that paragraph from Investigatory to Investigative.

Page 354:

Rule 2 MCAR § 1.209. The first sentence in the introductory paragraph should read: "Pursuant to Minn. Stat. § 15.1641 (d), ..."

Page 355:

Rule 2 MCAR § 1.210, the fourth paragraph should be denominated as D. instead of B.