

laid over

**Senators Ranum, Chaudhary, Skoglund and Ortman introduced—
S.F. No. 2951: Referred to the Committee on Judiciary.**

A bill for an act

1.2 relating to crimes; authorizing retention of certain juvenile history data for
1.3 purposes of predatory offender registration; amending Minnesota Statutes 2004,
1.4 section 299C.095, subdivision 2.

1.5 **BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:**

1.6 **Section 1. Minnesota Statutes 2004, section 299C.095, subdivision 2, is amended to**
1.7 **read:**

1.8 **Subd. 2. Retention. (a)** Notwithstanding section 138.17, the bureau shall retain
1.9 juvenile history records for the time periods provided in this subdivision. Notwithstanding
1.10 contrary provisions of paragraphs (b) to (e), all data in a juvenile history record must
1.11 be retained for the longest time period applicable to any item in the individual juvenile
1.12 history record. If, before data are destroyed under this subdivision, the subject of the
1.13 data is convicted of a felony as an adult, the individual's juvenile history record must be
1.14 retained for the same time period as an adult criminal history record.

1.15 **(b)** Juvenile history data on a child who was arrested must be destroyed six months
1.16 after the arrest if the child has not been referred to a diversion program and no petition has
1.17 been filed against the child by that time.

1.18 **(c)** Juvenile history data on a child against whom a delinquency petition was filed
1.19 and subsequently dismissed must be destroyed upon receiving notice from the court that
1.20 the petition was dismissed.

1.21 **(d)** Juvenile history data on a child who was referred to a diversion program or
2 against whom a delinquency petition has been filed and continued for dismissal must be
1.23 destroyed when the child reaches age 21.

2.1 (e) Juvenile history data on a child against whom a delinquency petition was filed
2.2 and continued without adjudication, or a child who was found to have committed a felony
2.3 or gross misdemeanor-level offense, must be destroyed when the child reaches age 28. If
2.4 the adjudication was for an offense which requires registration pursuant to section 243.166
2.5 or 243.167, or the offender commits a felony violation as an adult, the bureau shall retain
2.6 the data for as long as the data would have been retained if the offender had been an
2.7 adult at the time of the juvenile offense.

2.8 (f) The bureau shall retain extended jurisdiction juvenile data on an individual
2.9 received under section 260B.171, subdivision 2, paragraph (c), for as long as the data
2.10 would have been retained if the offender had been an adult at the time of the offense.

2.11 (g) Data retained on individuals under this subdivision are private data under section
2.12 13.02, except that extended jurisdiction juvenile data become public data under section
2.13 13.87, subdivision 2, when the juvenile court notifies the bureau that the individual's adult
2.14 sentence has been executed under section 260B.130, subdivision 5.

2.15 (h) A person who receives data on a juvenile under paragraphs (b) to (e) from the
2.16 bureau shall destroy the data according to the schedule in this subdivision, unless the
2.17 person has access to the data under other law. The bureau shall include a notice of the
2.18 destruction schedule with all data it disseminates on juveniles.

**Senate Counsel, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 2951 - BCA Juvenile History Records

Author: Senator Jane B. Ranum

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394) *K.P.*

Date: March 20, 2006

This bill amends the BCA juvenile history data record retention requirements to provide that if an adjudication was for an offense for which sex offender registration is required, the data must be retained for as long as if the offender had been an adult at the time of the juvenile offense.

KP:cs

1.1 To: Senator Betzold, Chair

1.2 Committee on Judiciary

Senator Skoglund,

1.4 Chair of the Subcommittee on Data Practices, to which was referred

1.5 **S.F. No. 2002:** A bill for an act relating to consumer protection; authorizing credit
 1.6 blocks in cases of identity theft; authorizing a consumer to place a security freeze on the
 1.7 consumer's credit report; providing notice of this right; providing protections against
 1.8 identity theft; providing Social Security number protections; providing credit monitoring;
 1.9 providing for the adequate destruction of personal records; providing civil and criminal
 1.10 penalties; proposing coding for new law in Minnesota Statutes, chapters 13C; 325E; 325G.

1.11 Reports the same back with the recommendation that the bill be amended as follows:

1.12 Page 1, after line 9, insert:

1.13 "Section 1. Minnesota Statutes 2004, section 13.6905, is amended by adding a
 1.14 subdivision to read:

1.15 Subd. 33. Victim of identity theft data. Data maintained by the Department of
 1.16 Public Safety that document victims of identity theft and determinations of innocence are
 1.17 classified under section 325E.66, subdivision 6."

1.18 Page 1, line 14, delete "his or her" and insert "the consumer's"

1.19 Page 2, lines 1 and 6, delete "he or she" and insert "the consumer"

1.20 Page 4, lines 30 and 32, delete "or entity"

1.21 Page 5, line 10, delete "....." and insert "Minnesota Statutes, section 13C.05."

1.22 Page 6, line 22, delete "government or governmental subdivision or agency,"

1.23 Page 6, line 29, delete everything after "parties"

1.24 Page 6, line 30, delete everything before the period

1.25 Page 7, line 13, delete "he"

1.26 Page 7, line 14, delete "or she" and insert "the person"

1.27 Page 7, line 16, delete "his or her" and insert "the person's"

1.28 Page 8, line 11, delete everything after the period

1.29 Page 8, delete lines 12 to 15 and insert "The data are private data on individuals as
 1.30 defined in section 13.02, subdivision 12. Law enforcement agencies have access to the
 1.31 data in order to assist victims of identify theft."

1.32 Page 8, line 34, delete "such" and insert "the"

1.33 Page 9, line 25, delete "his"

1.34 Page 9, line 26, delete "or her" and insert "the consumer's"

1.35 Page 10, line 13, delete "any such" and insert "the"

1.36 Page 11, line 2, delete "Such" and delete "may not be" and insert "are not"

1.37 Page 11, line 13, delete "and/or" and insert "or"

1.38 Page 11, line 23, delete "such" and insert "the"

1.39 Renumber the sections in sequence

2.1 Amend the title accordingly

2.2 And when so amended that the bill be recommended to pass and be referred to
2.3 the full committee.

2.4 
2.5 (Subcommittee Chair)

2.6 March 23, 2006
2.7 (Date of Subcommittee action)

A bill for an act
 relating to consumer protection; authorizing credit blocks in cases of identity
 theft; authorizing a consumer to place a security freeze on the consumer's credit
 report; providing notice of this right; providing protections against identity theft;
 providing Social Security number protections; providing credit monitoring;
 providing for the adequate destruction of personal records; providing civil and
 criminal penalties; proposing coding for new law in Minnesota Statutes, chapters
 13C; 325E; 325G.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [13C.032] IDENTITY THEFT; CREDIT BLOCKS.

(a) If a consumer submits to a credit reporting agency a copy of a valid police report, or a valid investigative report made by an investigator with peace officer status, the consumer credit reporting agency shall promptly and permanently block reporting any information that the consumer alleges appears on his or her credit report as a result of a violation of section 609.527 so that the information cannot be reported. The consumer credit reporting agency shall promptly notify the furnisher of the information that the information has been blocked. Furnishers of information and consumer credit reporting agencies shall ensure that information is unblocked only upon a preponderance of the evidence establishing the facts required under paragraph (b), clause (1), (2), or (3).

(b) The permanently blocked information must be unblocked only if:

(1) the information was blocked due to a material misrepresentation of fact by the consumer or fraud;

(2) the consumer agrees that the blocked information, or portions of the blocked information, were blocked in error; or

(3) the consumer knowingly obtained possession of goods, services, or money as a result of the blocked transaction or transactions or the consumer should have known

2.1 that he or she obtained possession of goods, services, or money as a result of the blocked
2.2 transaction or transactions.

2.3 (c) If blocked information is unblocked pursuant to this section, the consumer must
2.4 be promptly notified. The prior presence of the blocked information in the consumer
2.5 credit reporting agency's file on the consumer is not evidence of whether the consumer
2.6 knew or should have known that he or she obtained possession of any goods, services, or
2.7 money. For the purposes of this section, fraud may be demonstrated by circumstantial
2.8 evidence. In unblocking information pursuant to this section, furnishers and consumer
2.9 credit reporting agencies are subject to their respective requirements pursuant to this
2.10 chapter regarding the completeness and accuracy of information.

2.11 **Sec. 2. [13C.05] SECURITY FREEZE ON CONSUMER CREDIT REPORTS.**

2.12 **Subdivision 1. Definitions. For the purposes of this section, the following terms**
2.13 **have the meanings given them:**

2.14 **(1) "security freeze" means a notice, at the request of the consumer and subject to**
2.15 **certain exceptions, prohibiting the consumer reporting agency from releasing all or any**
2.16 **part of the consumer's credit report or any information derived from it without the express**
2.17 **authorization of the consumer. If a security freeze is in place, such a report or information**
2.18 **may not be released to a third party without prior express authorization from the consumer.**
2.19 **This subdivision does not prevent a consumer reporting agency from advising a third party**
2.20 **that a security freeze is in effect with respect to the consumer's credit report; and**

2.21 **(2) "reviewing the account" or "account review" includes activities related to account**
2.22 **maintenance, monitoring, credit line increases, and upgrades and enhancements.**

2.23 **Subd. 2. Timing; covered entities; cost. (a) A consumer may elect to place a**
2.24 **security freeze on a credit report by:**

2.25 **(1) making a request by certified mail;**

2.26 **(2) making a request by telephone by providing certain personal identification; or**

2.27 **(3) making a request directly to the consumer reporting agency through a secure**
2.28 **electronic mail connection if the connection is made available by the agency.**

2.29 **(b) A consumer reporting agency shall place a security freeze on a consumer's credit**
2.30 **report no later than five business days after receiving a written or telephone request from**
2.31 **the consumer or three business days after receiving a secure electronic mail request.**

2.32 **(c) The consumer reporting agency shall send a written confirmation of the security**
2.33 **freeze to the consumer within five business days of placing the freeze and at the same time**
2.34 **shall provide the consumer with a unique personal identification number or password to**

3.1 be used by the consumer when providing authorization for the release of the consumer's
3.2 credit for a specific party or period of time.

3.3 (d) If the consumer wishes to allow the consumer's credit report to be accessed for a
3.4 specific party or period of time while a freeze is in place, the consumer shall contact the
3.5 consumer reporting agency via telephone, certified mail, or secure electronic mail; request
3.6 that the freeze be temporarily lifted; and provide the following:

3.7 (1) proper identification;

3.8 (2) the unique personal identification number or password provided by the consumer
3.9 reporting agency pursuant to paragraph (c); and

3.10 (3) the proper information regarding the third party who is to receive the credit report
3.11 or the time period for which the report must be available to users of the credit report.

3.12 (e) A consumer reporting agency that receives a request from a consumer to
3.13 temporarily lift a freeze on a credit report pursuant to paragraph (d) shall comply with the
3.14 request no later than three business days after receiving the request.

3.15 (f) A consumer reporting agency may develop procedures involving the use of
3.16 telephone or fax, or upon the consent of the consumer in the manner required by the
3.17 Electronic Signatures in Global and National Commerce Act, United States Code, title 15,
3.18 section 7001 et seq., for legally required notices, by the Internet, e-mail, or other electronic
3.19 media to receive and process a request from a consumer to temporarily lift a freeze on a
3.20 credit report pursuant to paragraph (d) in an expedited manner.

3.21 (g) A consumer reporting agency shall remove or temporarily lift a freeze placed
3.22 on a consumer's credit report only in the following cases:

3.23 (1) upon consumer request, pursuant to paragraph (d) or (j); or

3.24 (2) if the freeze was due to a material misrepresentation of fact by the consumer.

3.25 If a consumer reporting agency intends to remove a freeze upon a consumer's credit report
3.26 pursuant to this paragraph, the consumer reporting agency shall notify the consumer in
3.27 writing five business days before removing the freeze on the consumer's credit report.

3.28 (h) If a third party requests access to a consumer credit report on which a security
3.29 freeze is in effect, and this request is in connection with an application for credit or any
3.30 other use, and the consumer does not allow the consumer's credit report to be accessed for
3.31 that specific party or period of time, the third party may treat the application as incomplete.

3.32 (i) If a third party requests access to a consumer credit report on which a security
3.33 freeze is in effect for the purpose of receiving, extending, or otherwise using the credit in
3.34 the report, and not for the sole purpose of account review, the consumer reporting agency
3.35 must notify the consumer that an attempt has been made to access the credit report.

- 4.1 (j) Except as otherwise provided in paragraph (g), clause (2), a security freeze shall
4.2 remain in place until the consumer requests that the security freeze be removed. A
4.3 consumer reporting agency shall remove a security freeze within three business days of
4.4 receiving a request for removal from the consumer, who provides both of the following:
- 4.5 (1) proper identification; and
4.6 (2) the unique personal identification number or password provided by the consumer
4.7 reporting agency pursuant to paragraph (c).
- 4.8 (k) A consumer reporting agency shall require proper identification of the person
4.9 making a request to place or remove a security freeze.
- 4.10 (l) A consumer reporting agency may not suggest or otherwise state or imply to a
4.11 third party that the consumer's security freeze reflects a negative credit score, history,
4.12 report, or rating.
- 4.13 (m) This section does not apply to the use of a consumer credit report by any of
4.14 the following:
- 4.15 (1) a person, or the person's subsidiary, affiliate, agent, or assignee with which
4.16 the consumer has or, prior to assignment, had an account, contract, or debtor-creditor
4.17 relationship for the purposes of reviewing the account or collecting the financial obligation
4.18 owing for the account, contract, or debt;
- 4.19 (2) a subsidiary, affiliate, agent, assignee, or prospective assignee of a person to
4.20 whom access has been granted under paragraph (d) for purposes of facilitating the
4.21 extension of credit or other permissible use;
- 4.22 (3) any person acting pursuant to a court order, warrant, or subpoena;
4.23 (4) a state or local agency which administers a program for establishing and
4.24 enforcing child support obligations;
- 4.25 (5) the Department of Health or its agents or assigns acting to investigate fraud;
4.26 (6) the Department of Revenue or its agents or assigns acting to investigate or collect
4.27 delinquent taxes or unpaid court orders to fulfill any of its other statutory responsibilities;
- 4.28 (7) a person for the purpose of prescreening as defined by the federal Fair Credit
4.29 Reporting Act;
- 4.30 (8) any person or entity administering a credit file monitoring subscription service to
4.31 which the consumer has subscribed; and
- 4.32 (9) any person or entity for the purpose of providing a consumer with a copy of the
4.33 consumer's credit report upon the consumer's request.
- 4.34 (n) A consumer may not be charged for any security freeze services, including but
4.35 not limited to the placement or lifting of a security freeze. A consumer may be charged no
4.36 more than \$5 only if the consumer fails to retain the original personal identification number

5.1 given to the consumer by the agency, but the consumer may not be charged for a onetime
5.2 reissue of the same or a new personal identification number. The consumer may be charged
5.3 no more than \$5 for subsequent instances of loss of the personal identification number.

5.4 Subd. 3. Notice of rights. At any time that a consumer is required to receive a
5.5 summary of rights required under section 609 of the federal Fair Credit Reporting Act, the
5.6 following notice must be included:

5.7 "Minnesota Consumers Have the Right to Obtain a Security Freeze

5.8 You may obtain a security freeze on your credit report at no charge to protect your
5.9 privacy and ensure that credit is not granted in your name without your knowledge. You
5.10 have a right to place a "security freeze" on your credit report pursuant to

5.11 The security freeze will prohibit a consumer reporting agency from releasing any
5.12 information in your credit report without your express authorization or approval.

5.13 The security freeze is designed to prevent credit, loans, and services from being
5.14 approved in your name without your consent. When you place a security freeze on your
5.15 credit report, within five business days you will be provided a personal identification
5.16 number or password to use if you choose to remove the freeze on your credit report or
5.17 to temporarily authorize the release of your credit report for a specific party, parties, or
5.18 period of time after the freeze is in place. To provide that authorization, you must contact
5.19 the consumer reporting agency and provide all of the following:

5.20 (1) the unique personal identification number or password provided by the consumer
5.21 reporting agency;

5.22 (2) proper identification to verify your identity; and

5.23 (3) the proper information regarding the third party or parties who are to receive
5.24 the credit report or the period of time for which the report shall be available to users
5.25 of the credit report.

5.26 A consumer reporting agency that receives a request from a consumer to lift
5.27 temporarily a freeze on a credit report shall comply with the request no later than three
5.28 business days after receiving the request.

5.29 A security freeze does not apply to circumstances where you have an existing
5.30 account relationship and a copy of your report is requested by your existing creditor
5.31 or its agents or affiliates for certain types of account review, collection, fraud control,
5.32 or similar activities.

5.33 If you are actively seeking credit, you should understand that the procedures
5.34 involved in lifting a security freeze may slow your own application for credit. You should
5.35 plan ahead and lift a freeze, either completely if you are shopping around, or specifically
5.36 for a certain creditor, a few days before actually applying for new credit.

6.1 You have a right to bring a civil action against someone who violates your rights
6.2 under the credit reporting laws. The action can be brought against a consumer reporting
6.3 agency or a user of your credit report.

6.4 Subd. 4. Violations; penalties. (a) If a consumer reporting agency erroneously,
6.5 whether by accident or design, violates the security freeze by releasing credit information
6.6 that has been placed under a security freeze, the affected consumer is entitled to:

6.7 (1) notification within five business days of the release of the information, including
6.8 specificity as to the information released and the third-party recipient of the information;

6.9 (2) file a complaint with the Federal Trade Commission, the state attorney general,
6.10 and the Department of Commerce; and

6.11 (3) in a civil action against the consumer reporting agency recover:

6.12 (i) injunctive relief to prevent or restrain further violation of the security freeze;

6.13 (ii) a civil penalty in an amount not to exceed \$10,000 for each violation plus any
6.14 damages available under other civil laws; and

6.15 (iii) reasonable expenses, court costs, investigative costs, and attorney fees.

6.16 (b) Each violation of the security freeze must be counted as a separate incident for
6.17 purposes of imposing penalties under this section.

6.18 **Sec. 3. [325E.65] DEFINITIONS.**

6.19 Subdivision 1. Scope. For the purposes of sections 325E.65 to 325E.67, the terms in
6.20 subdivisions 2 to 6 have the meanings given.

6.21 Subd. 2. Person. "Person" means any individual, partnership, corporation, trust,
6.22 estate, cooperative, association, government or governmental subdivision or agency,
6.23 or other entity.

6.24 Subd. 3. Consumer. "Consumer" means an individual.

6.25 Subd. 4. Consumer reporting agency. "Consumer reporting agency" means any
6.26 person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly
6.27 engages in whole or in part in the practice of assembling or evaluating consumer credit
6.28 information or other information on consumers for the purpose of furnishing consumer
6.29 reports to third parties, and which uses any means or facility of interstate commerce for
6.30 the purpose of preparing or furnishing consumer reports.

6.31 Subd. 5. Consumer report; credit report. "Consumer report" or "credit report"
6.32 means any written, oral, or other communication of any information by a consumer
6.33 reporting agency bearing on a consumer's creditworthiness, credit standing, credit
6.34 capacity, character, general reputation, personal characteristics, or mode of living which

7.1 is used or expected to be used or collected in whole or in part for the purpose of serving
7.2 as a factor in establishing the consumer's eligibility for:

7.3 (1) credit or insurance to be used primarily for personal, family, or household
7.4 purposes, except that nothing in sections 325E.65 to 325E.67 authorizes the use of credit
7.5 evaluations or credit scoring in the underwriting of personal lines of property or casualty
7.6 insurance;

7.7 (2) employment purposes; or

7.8 (3) any other purpose authorized under United States Code, title 15, section 1681b.

7.9 Subd. 6. Identity theft. "Identity theft" means theft, fraud, or attempted theft or
7.10 fraud committed using any identifying information of another person.

7.11 **Sec. 4. [325E.66] FACTUAL DECLARATION OF INNOCENCE AFTER**
IDENTITY THEFT.

7.12 Subdivision 1. Judicial determination. A person who reasonably believes that he
7.13 or she is the victim of identity theft may petition a court, or the court, on its own motion
7.14 or upon application of the prosecuting attorney, may move for an expedited judicial
7.15 determination of his or her factual innocence, where the perpetrator of the identity theft
7.16 was arrested for, cited for, or convicted of a crime under the victim's identity, or where a
7.17 criminal complaint has been filed against the perpetrator in the victim's name, or where
7.18 the victim's identity has been mistakenly associated with a record of criminal conviction.
7.19 Any judicial determination of factual innocence made pursuant to this section may be
7.20 heard and determined upon declarations, affidavits, police reports, or other material,
7.21 relevant, and reliable information submitted by the parties or ordered to be part of the
7.22 record by the court. Where the court determines that the petition or motion is meritorious
7.23 and that there is no reasonable cause to believe that the victim committed the offense for
7.24 which the perpetrator of the identity theft was arrested, cited, convicted, or subject to a
7.25 criminal complaint in the victim's name, or that the victim's identity has been mistakenly
7.26 associated with a record of criminal conviction, the court shall find the victim factually
7.27 innocent of that offense. If the victim is found factually innocent, the court shall issue an
7.28 order certifying this determination.

7.29 Subd. 2. Court order. After a court has issued a determination of factual innocence
7.30 pursuant to this section, the court may order the name and associated personal identifying
7.31 information contained in court records, files, and indexes accessible by the public
7.32 deleted, sealed, or labeled to show that the data is impersonated and does not reflect
7.33 the defendant's identity.
7.34

8.1 Subd. 3. Documentation. Upon making a determination of factual innocence, the
8.2 court must provide the consumer written documentation of such order.

8.3 Subd. 4. Vacating determination. A court that has issued a determination of
8.4 factual innocence pursuant to this section may at any time vacate that determination if
8.5 the petition, or any information submitted in support of the petition, is found to contain
8.6 any material misrepresentation or fraud.

8.7 Subd. 5. Form. The Supreme Court shall develop a form for use in issuing an order
8.8 pursuant to this section.

8.9 Subd. 6. Database. The Department of Public Safety shall establish and maintain a
8.10 database of individuals who have been victims of identity theft and that have received
8.11 determinations of factual innocence. The Department of Public Safety shall provide
8.12 a victim of identity theft or his or her authorized representative access to the database
8.13 in order to establish that the individual has been a victim of identity theft. Access to
8.14 the database shall be limited to criminal justice agencies, victims of identity theft, and
8.15 individuals and agencies authorized by the victims.

8.16 Sec. 5. [325E.67] CONSUMER-DRIVEN CREDIT MONITORING.

8.17 Subdivision 1. Disclosures. Every consumer credit reporting agency shall, upon
8.18 request from a consumer that is not covered by the free disclosures provided in United
8.19 States Code, title 15, section 1681j, subsections (a) to (d), clearly and accurately disclose
8.20 to the consumer:

8.21 (1) all information in the consumer's file at the time of the request, except that
8.22 nothing in this subdivision requires a consumer reporting agency to disclose to a consumer
8.23 any information concerning credit scores or other risk scores or predictors that are
8.24 governed by United States Code, title 15, section 1681g(f);

8.25 (2) the sources of the information;

8.26 (3) identification of each person, including each end-user identified under United
8.27 States Code, title 15, section 1681e, that procured a consumer report:

8.28 (i) for employment purposes, during the two-year period preceding the date on
8.29 which the request is made; or

8.30 (ii) for any purpose, during the one-year period preceding the date on which the
8.31 request is made;

8.32 (4) an identification of a person under clause (3) shall include:

8.33 (i) the name of the person or, if applicable, the trade name (written in full) under
8.34 which such person conducts business; and

8.35 (ii) upon request of the consumer, the address and telephone number of the person;

9.1 (5) clause (3) does not apply if:

9.2 (i) the end user is an agency or department of the United States government that
9.3 procures the report from the person for purposes of determining the eligibility of the
9.4 consumer to whom the report relates to receive access or continued access to classified
9.5 information (as defined in United States Code, title 15, section 1681b(b)(4)(E)(i)); and

9.6 (ii) the head of the agency or department makes a written finding as prescribed under
9.7 United States Code, title 15, section 1681b(b)(4)(A);

9.8 (6) the dates, original payees, and amounts of any checks upon which is based any
9.9 adverse characterization of the consumer, included in the file at the time of the disclosure
9.10 or which can be inferred from the file;

9.11 (7) a record of all inquiries received by the agency during the one-year period
9.12 preceding the request that identified the consumer in connection with a credit or insurance
9.13 transaction that was not initiated by the consumer;

9.14 (8) if the consumer requests the credit file and not the credit score, a statement that
9.15 the consumer may request and obtain a credit score.

9.16 Subd. 2. Cost of disclosure. In the case of a request under subdivision 1, a
9.17 consumer reporting agency may impose a reasonable charge on a consumer for making
9.18 a disclosure pursuant to this section, which charge must:

9.19 (1) not exceed \$3 for each of the first 12 requests from the consumer in a calendar
9.20 year;

9.21 (2) not exceed \$8 for any additional request beyond the initial 12 requests from the
9.22 consumer in a calendar year; and

9.23 (3) be indicated to the consumer before making the disclosure.

9.24 Subd. 3. Format of disclosure. In the case of a request under subdivision 1, a
9.25 consumer reporting agency must provide the consumer with an opportunity to access his
9.26 or her report through the following means:

9.27 (1) in writing;

9.28 (2) in person, upon the appearance of the consumer at the place of business of the
9.29 consumer reporting agency where disclosures are regularly provided, during normal
9.30 business hours, and on reasonable notice;

9.31 (3) by telephone, if the consumer has made a written request for disclosure;

9.32 (4) by electronic means, if the agency offers electronic access for any other purpose;

9.33 (5) by any other reasonable means that is available from the agency.

9.34 Subd. 4. Timing of disclosure. A consumer reporting agency shall provide a
9.35 consumer report under subdivision 1 no later than:

- 10.1 (1) 24 hours after the date on which the request is made, if the disclosure is made by
10.2 electronic means, as requested under subdivision 3, clause (4); and
10.3 (2) five days after the date on which the request is made, if the disclosure is made
10.4 in writing, in person, by telephone, or by any other reasonable means that is available
10.5 from the agency.

10.6 **Sec. 6. [325E.68] ADEQUATE DESTRUCTION OF PERSONAL RECORDS.**

10.7 Subdivision 1. Definitions. For the purposes of this section, the following terms
10.8 shall have the meanings given them:

10.9 (a) "Business" means sole proprietorship, partnership, corporation, association,
10.10 or other group, however organized and whether or not organized to operate at a profit.
10.11 The term includes a financial institution organized, chartered, or holding a license or
10.12 authorization certificate under the laws of this state, any other state, the United States, or
10.13 any other country, or the parent or the subsidiary of any such financial institution. The
10.14 term also includes an entity that destroys records.

10.15 (b) "Dispose" includes:

- 10.16 (1) the discarding or abandonment of records containing personal information; and
10.17 (2) the sale, donation, discarding, or transfer of any medium, including computer
10.18 equipment, or computer media, containing records of personal information, or other
10.19 nonpaper media upon which records of personal information is stored, or other equipment
10.20 for nonpaper storage of information.

10.21 (c) "Personal information" means any information that identifies, relates to,
10.22 describes, or is capable of being associated with a particular individual, including, but
10.23 not limited to, a name, signature, Social Security number, fingerprint, photograph or
10.24 computerized image, physical characteristics or description, address, telephone number,
10.25 passport number, driver's license or state identification card number, date of birth, medical
10.26 information, bank account number, credit card number, debit card number, or any other
10.27 financial information.

10.28 (d) "Records" means any material on which written, drawn, spoken, visual, or
10.29 electromagnetic information is recorded or preserved, regardless of physical form or
10.30 characteristics. "Records" does not include publicly available directories containing
10.31 information an individual has voluntarily consented to have publicly disseminated or
10.32 listed, such as name, address, or telephone number.

10.33 Subd. 2. Disposal of records containing personal information. Any business that
10.34 conducts business in Minnesota and any business that maintains or otherwise possesses
10.35 personal information of residents of Minnesota must take all reasonable measures to

11.1 protect against unauthorized access to or use of the information in connection with, or
11.2 after its disposal. Such reasonable measures must include, but may not be limited to:

11.3 (1) implementing and monitoring compliance with policies and procedures that
11.4 require the burning, pulverizing, or shredding of papers containing personal information
11.5 so that the information cannot practicably be read or reconstructed;

11.6 (2) implementing and monitoring compliance with policies and procedures that
11.7 require the destruction or erasure of electronic media and other nonpaper media containing
11.8 personal information so that the information cannot practicably be read or reconstructed;

11.9 (3) after due diligence, entering into and monitoring compliance with a written
11.10 contract with another party engaged in the business of record destruction to dispose of
11.11 personal information in a manner consistent with this statute. Due diligence should
11.12 ordinarily include, but may not be limited to, one or more of the following: reviewing an
11.13 independent audit of the disposal company's operations and/or its compliance with this
11.14 statute or its equivalent; obtaining information about the disposal company from several
11.15 references or other reliable sources and requiring that the disposal company be certified by
11.16 a recognized trade association or similar third party with a reputation for high standards
11.17 of quality review; reviewing and evaluating the disposal company's information security
11.18 policies or procedures; or taking other appropriate measures to determine the competency
11.19 and integrity of the disposal company; and

11.20 (4) for disposal companies explicitly hired to dispose of records containing personal
11.21 information: implementing and monitoring compliance with policies and procedures that
11.22 protect against unauthorized access to or use of personal information during or after
11.23 the collection and transportation and disposing of such information in accordance with
11.24 clauses (1) and (2).

11.25 Subd. 3. **Business policy.** Procedures relating to the adequate destruction or proper
11.26 disposal of personal records must be comprehensively described and classified as official
11.27 policy in the writings of the business entity, including corporate and employee handbooks
11.28 and similar corporate documents.

11.29 Subd. 4. **Penalties and civil liability.** (a) Any person or business that violates this
11.30 section is subject to a civil penalty of not more than \$3,000.

11.31 (b) Any individual aggrieved by a violation may bring a civil action in district
11.32 court to enjoin further violations and to recover actual damages, costs, and reasonable
11.33 attorney fees.

11.34 Sec. 7. **[325G.052] CREDIT CARD OFFERS AND SOLICITATIONS; ADDRESS**
11.35 **VERIFICATIONS.**

12.1 (a) A credit card issuer that mails an offer or solicitation to receive a credit card and,
12.2 in response, receives a completed application for a credit card that lists an address that is
12.3 different from the address on the offer or solicitation shall verify the change of address
12.4 before issuing a credit card.

12.5 (b) Notwithstanding any other provision of law, a person to whom an offer or
12.6 solicitation to receive a credit card is made is not liable for the unauthorized use of a credit
12.7 card issued in response to that offer or solicitation if the credit card issuer does not verify
12.8 the change of address before issuing a credit card.

12.9 (c) When a credit card issuer receives a written or oral request for a change of the
12.10 cardholder's billing address and then receives a written or oral request for an additional
12.11 credit card within ten days after the requested address change, the credit card issuer shall
12.12 not mail the requested additional credit card to the new address or, alternatively, activate
12.13 the requested additional credit card, unless the credit card issuer has verified the change
12.14 of address.

1.1 Senator Betzold moves to amend the Report of the Subcommittee on Data
1.2 Practices (SS2002SUB) to S.F. No. 2002 as follows:

1.3 Page 1, after line 9, insert:

1.4 "Section 1. Minnesota Statutes 2004, section 13.6905, is amended by adding a
1.5 subdivision to read:

1.6 Subd. 33. Victim of identity theft data. Data maintained by the Department of
1.7 Public Safety that document victims of identity theft and determinations of innocence are
1.8 classified under section 325E.66, subdivision 6."

1.9 Page 6, line 22, delete "government or governmental subdivision or agency,"

1.10 Page 8, line 11, delete everything after the period

1.11 Page 8, delete lines 12 to 15 and insert "The data are private data on individuals as
1.12 defined in section 13.02, subdivision 12. Law enforcement agencies have access to the
1.13 data in order to assist victims of identify theft."

1.14 Renumber the sections in sequence and correct the internal references

1.15 Amend the title accordingly

- 1.1 Senator moves to amend S.F. No. 2002 as follows:
- 1.2 Page 1, line 14, delete "his or her" and insert "the consumer's"
- 1.3 Page 2, lines 1 and 6, delete "he or she" and insert "the consumer"
- 1.4 Page 4, lines 30 and 32, delete "or entity"
- 1.5 Page 5, line 10, delete "....." and insert "Minnesota Statutes, section 13C.05"
- 1.6 Page 6, line 29, delete everything after "parties"
- 1.7 Page 6, line 30, delete everything before the period
- 1.8 Page 7, line 13, delete "he"
- 1.9 Page 7, line 14, delete "or she" and insert "the person"
- 1.10 Page 7, line 16, delete "his or her" and insert "the person's"
- 1.11 Page 8, line 12, delete "his or her" and insert "the victim's"
- 1.12 Page 8, line 34, delete "such" and insert "the"
- 1.13 Page 9, line 25, delete "his"
- 1.14 Page 9, line 26, delete "or her" and insert "the consumer's"
- 1.15 Page 10, line 13, delete "any such" and insert "the"
- 1.16 Page 11, line 2, delete "Such" and delete "may not be" and insert "are not"
- 1.17 Page 11, line 13, delete "and/or" and insert "or"
- 1.18 Page 11, line 23, delete "such" and insert "the"

1.1 To: Senator Betzold, Chair

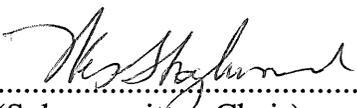
1.2 Committee on Judiciary

1.3 Senator Skoglund,

1.4 Chair of the Subcommittee on Data Practices, to which was referred

1.5 **S.F. No. 2965:** A bill for an act relating to consumer protection; regulating
1.6 the disclosure of personal information by data warehouses; providing notice content
1.7 requirements; removing an exemption for financial institutions and health care
1.8 entities; amending Minnesota Statutes 2005 Supplement, section 325E.61, subdivision 1,
1.9 by adding a subdivision; repealing Minnesota Statutes 2005 Supplement, section 325E.61,
1.10 subdivision 4.

1.11 Reports the same back with the recommendation that the bill do pass and be referred
1.12 to the full committee.

1.13 
1.14
(Subcommittee Chair)

1.15 March 23, 2006
1.16 (Date of Subcommittee action)

**Senators Chaudhary and Skoglund introduced—
S.F. No. 2965: Referred to the Committee on Judiciary.**

A bill for an act
relating to consumer protection; regulating the disclosure of personal information
by data warehouses; providing notice content requirements; removing an
exemption for financial institutions and health care entities; amending Minnesota
Statutes 2005 Supplement, section 325E.61, subdivision 1, by adding a
subdivision; repealing Minnesota Statutes 2005 Supplement, section 325E.61,
subdivision 4.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2005 Supplement, section 325E.61, subdivision 1, is
amended to read:

Subdivision 1. Disclosure of personal information; notice required. (a) Any
person or business that conducts business in this state, and that owns or licenses data that
includes personal information, shall disclose any breach of the security of the system
following discovery or notification of the breach in the security of the data to any resident
of this state whose unencrypted personal information was, or is reasonably believed to
have been, acquired by an unauthorized person. The disclosure must be made in the most
expedient time possible and without unreasonable delay, consistent with the legitimate
needs of law enforcement, as provided in paragraph (c), or with any measures necessary
to determine the scope of the breach, identify the individuals affected, and restore the
reasonable integrity of the data system.

(b) Any person or business that maintains data that includes personal information
that the person or business does not own shall notify the owner or licensee of the
information of any breach of the security of the data immediately following discovery,
if the personal information was, or is reasonably believed to have been, acquired by
an unauthorized person.

2.1 (c) The notification required by this section may be delayed to a date certain if a law
2.2 enforcement agency affirmatively determines that the notification will impede a criminal
2.3 investigation.

2.4 (d) For purposes of this section, "breach of the security of the system" means
2.5 unauthorized acquisition of computerized data that compromises the security,
2.6 confidentiality, or integrity of personal information maintained by the person or business.
2.7 Good faith acquisition of personal information by an employee or agent of the person or
2.8 business for the purposes of the person or business is not a breach of the security system,
2.9 provided that the personal information is not used or subject to further unauthorized
2.10 disclosure.

2.11 (e) For purposes of this section, "personal information" means an individual's first
2.12 name or first initial and last name in combination with any one or more of the following
2.13 data elements, when either the name or the data elements is not encrypted or is encrypted
2.14 with an encryption key that was also acquired:

2.15 (1) Social Security number;

2.16 (2) driver's license number or Minnesota identification card number; ~~or~~

2.17 (3) account number or credit or debit card number, in combination with any required
2.18 security code, access code, or password that would permit access to an individual's
2.19 financial account;

2.20 (4) account passwords, personal identification numbers, or other access codes; or

2.21 (5) biometric data. For purposes of this clause, "biometric data" means biological
2.22 data derived from direct measurement of a part of the human body. Direct measurement
2.23 technologies include, but are not limited to, fingerprinting, iris recognition, hand geometry,
2.24 and facial recognition.

2.25 (f) For purposes of this section, "personal information" does not include publicly
2.26 available information that is lawfully made available to the general public from federal,
2.27 state, or local government records.

2.28 (g) For purposes of this section, "notice" may be provided by one of the following
2.29 methods:

2.30 (1) written notice to the most recent available address the person or business has
2.31 in its records;

2.32 (2) electronic notice, if the notice provided is consistent with the provisions
2.33 regarding electronic records and signatures in United States Code, title 15, section 7001; or

2.34 (3) substitute notice, if the person or business demonstrates that the cost of providing
2.35 notice would exceed \$250,000, or that the affected class of subject persons to be notified

3.1 exceeds 500,000, or the person or business does not have sufficient contact information.

3.2 Substitute notice must consist of all of the following:

3.4 (i) e-mail notice when the person or business has an e-mail address for the subject persons;

3.5 (ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

3.6 (iii) notification to major statewide media.

3.7 (h) Notwithstanding paragraph (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing and content requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

3.14 Sec. 2. Minnesota Statutes 2005 Supplement, section 325E.61, is amended by adding a subdivision to read:

3.15 Subd. 1a. Content of notice. The notice required by this section must be clear and conspicuous. The notice must include:

3.16 (a) to the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including Social Security numbers, driver's license or state identification numbers, and financial data;

3.17 (b) the steps taken by the person or business to protect personal information from further unauthorized access;

3.18 (c) a toll-free telephone number:

3.19 (1) that the individual may use to contact a live representative of the agency or person; and

3.20 (2) from whom the individual may learn:

3.21 (i) what types of information the agency or person maintained about that individual or about individuals in general; and

3.22 (ii) whether the agency or person maintained information about that individual;

3.23 (d) the toll-free telephone numbers and addresses for the major consumer reporting agencies, along with a description of, and an explanation of how to exercise, the following rights under the federal Fair Credit Reporting Act:

3.24 (1) the right to obtain a credit report free of charge from each nationwide credit reporting agency;

4.1 (2) the right to place a fraud alert in consumer reports to put creditors on notice that
4.2 the individual may be a victim of fraud; and

4.3 (3) the right to block or delete specific items in consumer reports relating to
4.4 fraudulent transactions; and

4.5 (e) the toll-free telephone number and Web site address of the Federal Trade
4.6 Commission, along with a recommendation that the individual should report any incidents
4.7 of identity theft to a local law enforcement agency and the Federal Trade Commission.

4.8 **Sec. 3. REPEALER.**

4.9 Minnesota Statutes 2005 Supplement, section 325E.61, subdivision 4, is repealed.

APPENDIX
Repealed Minnesota Statutes: 06-5600

325E.61 DATA WAREHOUSES; NOTICE REQUIRED FOR CERTAIN DISCLOSURES.

Subd. 4. **Exemption.** This section does not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3), and to entities subject to the federal privacy and security regulations adopted under the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

Senator Skoglund introduced—

S.F. No. 3132: Referred to the Committee on Judiciary.

A bill for an act

relating to data practices; proposing classifications of data as private and nonpublic; amending Minnesota Statutes 2004, section 13.3805, by adding a subdivision.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2004, section 13.3805, is amended by adding a subdivision to read:

Subd. 4. Drinking water testing data. All data maintained by the Department of Health or community public water systems that identify the address of the testing site and the name, address, and telephone number of residential homeowners of each specific site that is tested for lead and copper as required by the federal Safe Drinking Water Act, the United States Environmental Protection Agency's lead and copper rule, and the department's drinking water protection program are classified as private data on individuals and nonpublic data.

1.1 Senator moves to amend S.F. No. 3132 as follows:

1.2 Page 2, after line 14, insert:

1.3 "Sec. 2. Minnesota Statutes 2005 Supplement, section 270C.03, subdivision 1,
1.4 is amended to read:

1.5 Subdivision 1. **Powers and duties.** The commissioner shall have and exercise
1.6 the following powers and duties:

1.7 (1) administer and enforce the assessment and collection of taxes;

1.8 (2) make determinations, corrections, and assessments with respect to taxes,
1.9 including interest, additions to taxes, and assessable penalties;

1.10 (3) use statistical or other sampling techniques consistent with generally accepted
1.11 auditing standards in examining returns or records and making assessments;

1.12 (4) investigate the tax laws of other states and countries, and formulate and submit
1.13 to the legislature such legislation as the commissioner may deem expedient to prevent
1.14 evasions of state revenue laws and to secure just and equal taxation and improvement in
1.15 the system of state revenue laws;

1.16 (5) consult and confer with the governor upon the subject of taxation, the
1.17 administration of the laws in regard thereto, and the progress of the work of the
1.18 department, and furnish the governor, from time to time, such assistance and information
1.19 as the governor may require relating to tax matters;

1.20 (6) execute and administer any agreement with the secretary of the treasury or the
1.21 Bureau of Alcohol, Tobacco, Firearms, and Explosives in the Department of Justice of the
1.22 United States or a representative of another state regarding the exchange of information
1.23 and administration of the state revenue laws;

1.24 (7) require town, city, county, and other public officers to report information as to the
1.25 collection of taxes received from licenses and other sources, and such other information
1.26 as may be needful in the work of the commissioner, in such form as the commissioner
1.27 may prescribe;

1.28 (8) authorize the use of unmarked motor vehicles to conduct seizures or criminal
1.29 investigations pursuant to the commissioner's authority; and

1.30 (9) exercise other powers and authority and perform other duties required of or
1.31 imposed upon the commissioner by law."

1.32 Amend the title accordingly

add immediate effective date

- 1.1 Senator moves to amend S.F. No. 3132 as follows:
- 1.2 Page 1, line 8, delete "All"
- 1.3 Page 1, line 13, delete "classified as"
- 1.4 Page 14, delete "and" and insert "or"

1.1 Senator moves to amend S.F. No. 3132 as follows:

1.2 Page 1, after line 5, insert:

1.3 "Section 1. Minnesota Statutes 2004, section 13.32, is amended by adding a
1.4 subdivision to read:

1.5 Subd. 8a. Access by juvenile justice system; bullying behavior. (a) For purposes
1.6 of this subdivision, "bullying behavior" means any written or verbal expression or physical
1.7 act or gesture by a student that is intended to cause or is perceived as causing distress to
1.8 one or more students and that substantially interferes with another student's educational
1.9 benefits, opportunities, or performance. Bullying includes, but is not limited to, conduct
1.10 by a student against another student that a reasonable person under the circumstances
1.11 knows or should know has the effect of harming a student, damaging a student's property,
1.12 placing a student in reasonable fear of harm to the student's person or property, or creating
1.13 a hostile educational environment for a student.

1.14 (b) Education data relating to bullying behavior by a student may be disclosed
1.15 under subdivision 3, clause (i)."

1.16 Renumber the sections in sequence and correct the internal references

1.17 Amend the title accordingly

72020000

Senators Ranum, Chaudhary, Skoglund and Ortman introduced—
S.F. No. 2950: Referred to the Committee on Judiciary.

A bill for an act
relating to data practices; classifying name and event index service of the Bureau
of Criminal Apprehension; amending Minnesota Statutes 2004, section 13.87, by
adding a subdivision.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2004, section 13.87, is amended by adding a subdivision
to read:

Subd. 4. Name and index service; data classification. Data collected, created, or
maintained by the name and event index service of the Bureau of Criminal Apprehension
are classified as private data, pursuant to section 13.02, subdivision 12, and become
confidential data, pursuant to section 13.02, subdivision 3, when the data joins private or
public data to any confidential data.

1.1 Senator moves to amend S.F. No. 2950 as follows:

1.2 Delete everything after the enacting clause and insert:

1.3 "Section 1. Minnesota Statutes 2004, section 13.87, is amended by adding a
1.4 subdivision to read:

1.5 Subd. 4. Name and index service data. (a) For purposes of this section, "name
1.6 and event index service data" means data of the Bureau of Criminal Apprehension that
1.7 link data on an individual that are stored in one or more databases maintained by criminal
1.8 justice agencies, as defined in section 299C.46, subdivision 2, or the judiciary.

1.9 (b) Name and event index service data are private data on individuals, provided
1.10 that if the data link private or public data on an individual to confidential data on that
1.11 individual, the data are confidential data on that individual. The data become private data
1.12 if the data no longer link private or public data to confidential data. The classification of
1.13 data in the name and event index service does not change the classification of the data in
1.14 the databases linked by the service."

1.15 Amend the title accordingly

Senator Skoglund introduced—

S.F. No. 2813: Referred to the Committee on Judiciary.

1.1 A bill for an act
1.2 relating to government data practices; providing for disclosure and sharing of
1.3 certain data; amending Minnesota Statutes 2004, section 626.557, subdivision 9a.

1.4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

1.5 Section 1. Minnesota Statutes 2004, section 626.557, subdivision 9a, is amended to
1.6 read:

1.7 Subd. 9a. **Evaluation and referral of reports made to a common entry**
1.8 **point unit.** The common entry point must screen the reports of alleged or suspected
1.9 maltreatment for immediate risk and make all necessary referrals as follows:

1.10 (1) if the common entry point determines that there is an immediate need for
1.11 adult protective services, the common entry point agency shall immediately notify the
1.12 appropriate county agency;

1.13 (2) if the report contains suspected criminal activity against a vulnerable adult, the
1.14 common entry point shall immediately notify the appropriate law enforcement agency;

1.15 (3) if the report references alleged or suspected maltreatment and there is no
1.16 immediate need for adult protective services, the common entry point shall notify the
1.17 appropriate lead agency as soon as possible, but in any event no longer than two working
1.18 days;

1.19 (4) if the report does not reference alleged or suspected maltreatment, the common
1.20 entry point may determine whether the information will be referred; and

1.21 (5) if the report contains information about a suspicious death, the common entry
1.22 point shall immediately notify the appropriate law enforcement agencies, the local medical
1.23 examiner, and the ombudsman established under section 245.92. Law enforcement

- 2.1 agencies shall coordinate with the local medical examiner and the ombudsman as provided
- 2.2 by law.

Senator Skoglund introduced—

S.F. No. 3041: Referred to the Committee on Judiciary.

1.1 A bill for an act
1.2 relating to data practices; clarifying the length of time allowed for giving notice;
1.3 amending Minnesota Statutes 2004, section 13.072, subdivision 1.

1.4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

1.5 Section 1. Minnesota Statutes 2004, section 13.072, subdivision 1, is amended to read:

1.6 Subdivision 1. **Opinion; when required.** (a) Upon request of a government entity,
1.7 the commissioner may give a written opinion on any question relating to public access
1.8 to government data, rights of subjects of data, or classification of data under this chapter
1.9 or other Minnesota statutes governing government data practices. Upon request of any
1.10 person who disagrees with a determination regarding data practices made by a government
1.11 entity, the commissioner may give a written opinion regarding the person's rights as a
1.12 subject of government data or right to have access to government data.

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

1.21 (c) If the commissioner determines that no opinion will be issued, the commissioner
1.22 shall give the government entity or body subject to chapter 13D or person requesting
1.23 the opinion notice of the decision not to issue the opinion within five business days of

2.1 receipt of the request. If this notice is not given, the commissioner shall issue an opinion
2.2 within 20 days of receipt of the request.

2.3 (d) For good cause and upon written notice to the person requesting the opinion,
2.4 the commissioner may extend this deadline for one additional 30-day period. The notice
2.5 must state the reason for extending the deadline. The government entity or the members
2.6 of a body subject to chapter 13D must be provided a reasonable opportunity to explain the
2.7 reasons for its decision regarding the data or how they perform their duties under chapter
2.8 13D. The commissioner or the government entity or body subject to chapter 13D may
2.9 choose to give notice to the subject of the data concerning the dispute regarding the data
2.10 or compliance with chapter 13D.

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

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

Senator Skoglund introduced—

S.F. No. 3042: Referred to the Committee on Judiciary.

1.1 A bill for an act
 1.2 relating to data practices; modifying records management requirements;
 1.3 changing emergency records preservation requirements; amending Minnesota
 1.4 Statutes 2004, section 138.17, subdivisions 7, 8.

1.5 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

1.6 Section 1. Minnesota Statutes 2004, section 138.17, subdivision 7, is amended to read:

1.7 Subd. 7. **Records management program.** ~~A records management program for the~~
 1.8 ~~application of efficient and economical management methods to the creation, utilization,~~
 1.9 ~~maintenance, retention, preservation, and disposal of official records shall be administered~~
 1.10 ~~by the commissioner of administration with assistance from the director of the historical~~
 1.11 ~~society. The State Records Center which stores and services state records not in state~~
 1.12 ~~archives shall be administered by the commissioner of administration. The commissioner~~
 1.13 ~~of administration is empowered to (1) establish standards, procedures, and techniques for~~
 1.14 ~~effective management of government records, (2) make continuing surveys of paper work~~
 1.15 ~~operations, and (3) recommend improvements in current records management practices~~
 1.16 ~~including the use of space, equipment, and supplies employed in creating, maintaining,~~
 1.17 ~~preserving and disposing of government records. It shall be the duty of the head of each~~
 1.18 ~~state agency and the governing body of each county, municipality, and other subdivision~~
 1.19 ~~of government to cooperate with the commissioner in conducting surveys and to establish~~
 1.20 ~~and maintain an active, continuing program for the economical and efficient management~~
 1.21 ~~of the records of each agency, county, municipality, or other subdivision of government.~~
 1.22 ~~When requested by the commissioner, Public officials shall assist in the preparation of~~
 1.23 prepare an inclusive inventory of records in their custody, to which shall be attached
 1.24 a schedule, approved by the head of the governmental unit or agency having custody

2.1 of the records ~~and the commissioner~~, establishing a time period for the retention or
2.2 disposal of each series of records. When the schedule is unanimously approved by the
2.3 records disposition panel, the head of the governmental unit or agency having custody
2.4 of the records may dispose of the type of records listed in the schedule at a time and in
2.5 a manner prescribed in the schedule for particular records which were created after the
2.6 approval. A list of records disposed of pursuant to this subdivision shall be maintained by
2.7 the governmental unit or agency.

2.8 Sec. 2. Minnesota Statutes 2004, section 138.17, subdivision 8, is amended to read:

2.9 Subd. 8. **Emergency records preservation.** ~~In light of the danger of nuclear or~~
2.10 ~~natural disaster, the commissioner of administration, with the assistance of the director~~
2.11 ~~of the historical society, shall establish and maintain a program for the selection and~~
2.12 ~~preservation of public records considered essential to the operation of government and to~~
2.13 ~~the protection of the rights and interests of persons, and shall make or cause to be made~~
2.14 ~~preservation duplicates or designate as preservation duplicates existing copies of such~~
2.15 ~~essential public records. Preservation duplicates shall be durable, accurate, complete, and~~
2.16 ~~clear, and such duplicates reproduced by photographic or other process which accurately~~
2.17 ~~reproduces and forms a durable medium for so reproducing the original shall have the~~
2.18 ~~same force and effect for all purposes as the original record whether the original record is~~
2.19 ~~in existence or not. A transcript, exemplification, or certified copy of such preservation~~
2.20 ~~duplicate shall be deemed for all purposes to be a transcript, exemplification, or certified~~
2.21 ~~copy of the original record. Such preservation duplicates shall be preserved in the place~~
2.22 ~~and manner of safekeeping prescribed by the commissioner.~~

2.23 Every county, municipality, or other subdivision of government may institute
2.24 a program for the preservation of necessary documents essential to the continuity of
2.25 government in the event of a disaster or emergency. ~~Such a program shall first be~~
2.26 ~~submitted to the commissioner for approval or disapproval and no such program shall be~~
2.27 ~~instituted until such approval is obtained.~~

1.1 A bill for an act
1.2 relating to health; modifying access to health care records; amending Minnesota
1.3 Statutes 2004, section 144.335, by adding a subdivision.

1.4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

1.5 Section 1. Minnesota Statutes 2004, section 144.335, is amended by adding a
1.6 subdivision to read:

1.7 **Subd. 3d. Release of records for family and caretaker involvement in mental**
1.8 **health care. (a) Notwithstanding subdivision 3a, a provider providing mental health care**
1.9 **and treatment may disclose health record information described in paragraph (b) about a**
1.10 **patient to a family member of the patient or other person who requests the information if:**

1.11 **(1) the request for information is in writing;**

1.12 **(2) the family member or other person lives with, provides care for, or is directly**
1.13 **involved in monitoring the treatment of the patient;**

1.14 **(3) the involvement under clause (2) is verified by the patient's mental health care**
1.15 **provider, the patient's attending physician, or a person other than the person requesting**
1.16 **the information;**

1.17 **(4) before the disclosure, the patient is informed in writing of the request, the name**
1.18 **of the person requesting the information, the reason for the request, and the specific**
1.19 **information being requested;**

1.20 **(5) the patient agrees to the disclosure, does not object to the disclosure, or is unable**
1.21 **to consent or object; and**

1.22 **(6) the disclosure is necessary to assist in the provision of care or monitoring of the**
1.23 **patient's treatment.**

2.1 (b) The information disclosed under this subdivision is limited to diagnosis,
2.2 admission to or discharge from treatment, the name and dosage of the medications
2.3 prescribed, side effects of the medication, consequences of failure of the patient to take the
2.4 prescribed medication, and a summary of the discharge plan.

2.5 (c) If a provider reasonably determines that providing information under this
2.6 subdivision would be detrimental to the physical or mental health of the patient or is
2.7 likely to cause the patient to inflict self harm or to harm another, the provider must not
2.8 disclose the information.

2.9 (d) This subdivision does not apply to disclosures for a medical emergency or to
2.10 family members as authorized or required under subdivision 3a, paragraph (b), clause
2.11 (1), or paragraph (f).

**Senate Counsel, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 2950 - BCA Name and Event Index Data

Author: Senator Jane B. Ranum

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394) *K.P.*

Date: March 20, 2006

This bill classifies name and index service data maintained by the Bureau of Criminal Apprehension as private data, except that if the data join private or public data to confidential data, the data become confidential data.

KP:cs

**Senate Counsel, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 2002 - Consumer Identity Theft Protections

Author: Senator Dan Sparks

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394)

Date: March 20, 2006

This bill contains a number of provisions to protect consumers from identity theft.

Section 1 establishes a procedure for blocking information in a consumer credit report that is alleged to appear as a result of a violation of section 609.527 (identify theft). The consumer must submit a police report or other investigative report regarding the alleged violation. Consumer credit reporting agencies must notify furnishers of information that it has been blocked. The circumstances under which information may be unblocked are specified. The consumer must be notified if information is unblocked. The legal effect of the prior presence of blocked information is specified.

Section 2 contains a process under which a consumer may place a security freeze on a credit report.

Subdivision 1 contains the definitions.

Subdivision 2 contains the process for a consumer to place a security freeze on a credit report. A consumer may allow the report to be given to a specific party or for a specific period of time while the freeze is in place. Consumer reporting agencies may develop procedures for receiving and processing requests to temporarily lift a freeze. Provisions are included dealing with the effect of third-party requests for access to a credit report on which a freeze is in effect. Exceptions to the freeze are included for specified entities. A consumer may not be charged for a security freeze.

Subdivision 3 requires a notice of the right to obtain a security freeze to be included as part of the summary of rights required under the federal Fair Credit Reporting Act and specifies the notice language.

Subdivision 4 governs violations, penalties, and remedies.

Sections 2 to 4 contain procedural protections and notices regarding identity theft.

Section 2 contains the definitions.

Section 4 authorizes a person who has learned or reasonably suspects that the person is a victim of identity theft, a court, or prosecuting attorney, to move for an expedited judicial determination of the facts if a perpetrator was arrested, cited for, or convicted of a crime involving the victim or the victim's name has been involved in a complaint or record of conviction. The court may find a victim factually innocent of the offense and issue an order certifying this determination. The court may also order that related information associated with the identify theft be removed from court records and other records accessible to the public. Provisions are included for documentation of an order, vacating a determination, the form, and the establishment of a database within the Department of Public Safety of individuals who have been victims of identity theft and have received a determination of factual innocence. Access to the database is limited to criminal justice agencies, victims, and individuals and agencies authorized by victims.

Section 5 establishes a procedure for consumer-driven monitoring of information in a credit report. Information that must be disclosed is specified and exceptions are included. Provisions are also included dealing with the cost of disclosure, format, and timing.

Section 6 establishes a process governing adequate destruction of personal records.

Subdivision 1 contains the definitions.

Subdivision 2 requires a business that conducts business in Minnesota and maintains or possess personal information of Minnesota residents to take reasonable measures to protect against unauthorized access or use of disposed information. Reasonable measures are specified.

Subdivision 3 requires these procedures to be part of business policy, such as corporate and employee handbooks and similar corporate documents.

Subdivision 4 contains the penalties and civil liability.

Section 7 regulates credit card offers and solicitations and contains address verification requirements. If the credit card issuer has not verified the address before issuing a credit card, the person to whom an offer was made is not liable for unauthorized use. Requirements are included governing situations where there is a request for a change in a billing address.

KP:cs

But, Identity Theft and Security Breaches Continue:

From Feb 15, 2006 to March 14, 2006, Businesses reported that over 53 million consumers' records have been exposed to potential and actual fraud cases reported

**National Survey on Data Security Breach Notification (9/05), By
Ponemon Institute**

- **Organizations most likely to report a breach are:**

Banks (20%),

Credit card companies (18%),

Governmental organizations (including state universities) (13%),

Health care providers (9%).

Remaining 40% other businesses

- **86% of security breaches involved the loss or theft of customer or consumer information. About 14% involved employee, student, medical and taxpayer data.**
- **58% Customer said the breach decreased their sense of trust and confidence in the organization reporting the incident. Only 8% of respondents did not blame the organization that reported the breach. Surprisingly, 12% said the incident enhanced their sense of confidence in the organization.**
- **Over 82% of customer believed that an organization should always report a breach, even if the lost or stolen data was encrypted or there was no criminal intent.**
- **59% of respondents don't have confidence in US state or federal regulation to protect them from data security breaches.**

**Senate Council, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 2965 - Data Warehouses

Author: Senator Satveer Chaudhary

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394) *K.P.*

Date: March 20, 2006

This bill contains amendments to the data warehouse privacy provisions enacted last session.

Section 1 amends the disclosure requirements in cases where there has been a breach of a security system to modify the definition of "personal information." It would include data elements that are encrypted if the encryption key was also acquired; account passwords, personal identification numbers, or other access codes; or biometric data.

Section 2 specifies the contents of a notice.

Section 3 repeals an exemption for certain financial institutions and entities subject to HIPAA (the federal medical records privacy law).

KP:cs

John Doe
1234 North Maple Lane
Nice Town, MN 55555
YOUR TAX ID NUMBER IS 472-55-1234
Your Birthday is 3/2/54
Your 401K Account number with FYZ Financial is: 12345678999
Hello:

I am sorry to tell you, but your identity has been stolen.

I used to work for FYZ Financial. They fired me for some bullshit reason so I am going to completely f* them over. Since they were so stupid and didn't bother to remove my mainframe system access or password, I knew how I was going to do it.**

A while back (after they F*** me over by firing me) I went back into their system and copied all the client information for a whole asslo*d of account (many thousand actually).**

I found someone who wanted to buy the list from me so I just sold it to them.....

**Senate Counsel, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 2813 - Vulnerable Adult Data

Author: Senator Wes Skoglund

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394)

K.P.

Date: March 20, 2006

This bill amends the data sharing provisions in the Vulnerable Adult Maltreatment Reporting Act to provide for the reporting of suspicious deaths to the local medical examiner, in addition to law enforcement and the ombudsman established under **section 245.92.**

KP:cs

**Senate Council, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 3042 - Records Management Requirements

Author: Senator Wes Skoglund

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394) *K.P.*

Date: March 20, 2006

This bill amends records management requirements of the Commissioner of Administration.

Section 1 strikes a requirement that the Commissioner of Administration administer a records management program but retains the requirements that state agencies and local governments have programs in place.

Section 2 eliminates a requirement that the Commissioner of Administration, with the assistance the director of the Minnesota Historical Society, establish and maintain a program for the selection and preservation of public records considered essential to the operation of government and to the protection of the rights and interests of persons. Local government requirements with respect to preserving necessary documents essential to the continuity of government in the event of a disaster or emergency would continue.

KP:cs

MINNESOTA DEPARTMENT OF ADMINISTRATION PROPOSED REPEAL OF RECORDS MANAGEMENT DUTIES SF 3042(Skoglund)/HF 3868(Holberg)

What is “records management?”

Records management is the orderly disposition of government records, usually according to a pre-approved plan known as a records retention schedule. A records retention schedule is prepared and submitted to the records disposition panel (Historical Society, auditor, attorney general) for approval so that a government entity can dispose of records. Without an approved records retention schedule, government records cannot be destroyed or transferred.

General records retention schedules that cover most records of a government entity have been developed for state agencies, counties, cities, school districts and townships and can be adopted and used by those units of government.

Administration’s role in records management

Historically, the Department of Administration provided assistance to state and local government units in the preparation of records retention schedules and answered questions about appropriate destruction and handling of government records.

Most recently, the function was housed within the Department’s Information Policy Analysis Division (IPAD). In 2002, then Commissioner David Fisher decided to cut the remaining \$70,000 (1 FTE) allocated to the function and IPAD stopped providing services.

This proposal

This proposal will align statutes with current practice. The proposed language repeals the duties that have been assigned to the Commissioner of Administration in Minnesota Statutes Section 138.17.

Resources available

Most local units of government have been receiving assistance from their associations and two of the four general records retention schedules are available on the Internet.

State agencies must rely on their internal records managers for assistance with these issues.

The State Archives Department at the Minnesota Historical Society serves as the secretary to the records disposition panel and is the custodian of the approved records retention schedules and other documents that authorize records destruction.

Contact information

Laurie Beyer-Kropuenske, Director of IPAD, 651-201-2501, laurie.beyer-kropuenske@state.mn.us
Katie Engler, Assistant Director, 651-201-2503, katherine.a.engler@state.mn.us

**Senate Counsel, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 3041 - Commissioner's Opinions

Author: Senator Wes Skoglund

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394) *K.P.*

Date: March 20, 2006

This bill clarifies the statute dealing with the issuance of data practices opinions by the Commissioner of Administration to provide that if the Commissioner determines that an opinion will not be issued, notice must be given to the requestor of this decision within five business days of the receipt of the request.

KP:cs

MINNESOTA DEPARTMENT OF ADMINISTRATION
PROPOSED ADVISORY OPINION CHANGE
SF 3041(Skoglund)/HF 3867(Holberg)

Advisory opinion authority

Under Minn. Stat. 13.072, the Commissioner of Administration has discretion to issue non-binding advisory opinions on data practices, open meeting law and other information policy statutes. Issues addressed in advisory opinion include public access, data classification, and rights of data subjects.

Opinion requests can be made by the public and government entities.

Statutory timeline for opinions

The Commissioner must:

- ◆ Reject an opinion request within 5 days from the date of receipt
- ◆ Issue an opinion within 20 days from receipt of request
- ◆ If one-time 30-day extension is exercised, issue an opinion within 50 days from receipt of request

Issue to be addressed

Advisory opinion requests require research and/or clarification from the requestor before they can be accepted or rejected. When a request is received before a weekend or a holiday, two or three days of research time and opportunity to contact the requestor for clarification is lost.

Proposed Change

This proposal would amend the timeframe the Commissioner has to reject a request for an advisory opinion from five days to five “business” days, which would exclude weekends and holidays.

Expected benefit

This proposal will ensure that the Commissioner has sufficient time to conduct more comprehensive research and contact requestors for clarifications before making a decision to accept or reject a request. Customer service will be improved as staff can provide more extensive responses when opinion requests are denied. When a request is denied, staff will provide information about existing opinions that address the issue presented on which the requestor can rely per Minn. Stat. 13.08 Subd. 4(b)(5).

Contact information

Laurie Beyer-Kropuenske, Director of IPAD, 651-201-2501, laurie.beyer-kropuenske@state.mn.us
Katie Engler, Assistant Director, 651-201-2503, katherine.a.engler@state.mn.us

Does the HIPAA Privacy Rule permit a doctor to discuss a patient's health status, treatment, or payment arrangements with the patient's family and friends?

Answer

Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient's mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient's payment options with her adult daughter.
- A doctor may instruct a patient's roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
- A physician may discuss a patient's treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

Even when the patient is not present or it is impracticable because of emergency circumstances or the patient's incapacity for the covered entity to ask the patient about discussing her care or payment with a family member or other person, a covered entity may share this information with the person when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b). Thus, for example:

- A surgeon may, if consistent with such professional judgment, inform a patient's spouse, who accompanied her husband to the emergency room, that the patient has suffered a heart attack and provide periodic updates on the patient's progress and prognosis.
- A doctor may, if consistent with such professional judgment, discuss an incapacitated patient's condition with a family member over the phone.

In addition, the Privacy Rule expressly permits a covered entity to use professional judgment and experience with common practice to make reasonable inferences about the patient's best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. For example, when a person comes to a pharmacy requesting to pick up a prescription on behalf of an individual he identifies by name, a pharmacist, based on professional judgment and experience with common practice, may allow the person to do so.

From the website of the U.S. Department of Health and Human Services

Support SF 1695 *The Family Involvement Bill*

Why this bill is needed:

When someone in your family is ill, you want to help them. It may mean driving them to appointments, preparing special meals, writing down information from doctors, keeping track of medications and even looking for side effects of medications. Typically, health care providers welcome a family's involvement and provide necessary information so that the family can in fact help care for their loved one.

When that illness is a mental illness, for some reason that door closes. Citing data privacy concerns, mental health care providers do not share information unless a signed privacy release is obtained. Often they say they wish they could share information, but again, without a release they cannot do that.

The reality is that few families are asking for access to their loved one's complete medical records. What they want is the basic information that will help them care for their loved one and be an advocate for them.

Families relate how no one will talk to them when their loved one is hospitalized, yet when it's time to discharge the person and a place cannot be found, the family gets that phone call.

What this bill would do:

This bill provides an alternative to full-blown access to medical records. It will permit mental health care providers to tell involved family members the basic information needed so that they can be good caregivers and advocates.

There are protections. It's not just any family member that can step in and obtain the information. He or she must have had a history of involvement and be living with or directly involved with monitoring treatment. The patient must be informed in writing of the request for information including who is requesting it and what information is being provided. The patient must agree or not object. The professional has some leeway in terms of professional judgment if he or she believes that providing the information would be detrimental to the patient.

The type of information that can be released is also limited. It is limited to diagnosis, admission to or discharge from treatment, the name of the medications prescribed, side effects of the medication, consequences of failure to take the prescribed medication and a summary of the discharge plan.

The HIPAA Privacy Rule at 45 CFR 164.510(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care.

NAMI Minnesota
800 Transfer Road, Suite 7A
St. Paul, MN 55114
651-645-2948

**Senate Counsel, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 3132 - Drinking Water Testing Data

Author: Senator Wes Skoglund

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394) *K.P.*

Date: March 20, 2006

This bill provides that data maintained by the Department of Health or community public water systems that identify the address of a site that is tested for lead and copper and the name, address, and telephone number of residential homeowners in the site, are private data or nonpublic data.

KP:cs

**Senate Counsel, Research,
and Fiscal Analysis**

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 1695 - Family and Caretaker Access to Mental Health Care Records (first engrossment)

Author: Senator Wes Skoglund

Prepared by: Kathleen Pontius, Senate Counsel (651/296-4394) *K.P.*

Date: March 20, 2006

This bill amends the medical records statute to authorize the release of records necessary for family and caretaker involvement in mental health care under certain circumstances. A provider would be authorized to disclose information about a patient to a family member or other person who requests the information if:

- (1) the request is in writing;
- (2) the person lives with, provides care for, or is directly involved in monitoring the patient's treatment;
- (3) the involvement is verified by the provider, the attending physician, or someone other than the person requesting the information;
- (4) before the disclosure, the patient is informed in writing of the request, the name of the requestor, the reason, and the information being requested;
- (5) the patient agrees to disclosure, does not object, or is unable to consent or object; and
- (6) the disclosure is necessary to assist in the provision of care or monitoring of the patient.

The information that may be disclosed is limited to diagnosis, admission to or discharge from treatment, name and dosage of medication, side effects, consequences of failure to take medication, and a summary of the discharge plan. If the provider reasonably determines that providing information would be detrimental to the health of the patient or is likely to cause the patient to inflict

self harm or harm to another, the provider must not disclose the information. This subdivision would not apply to disclosures for a medical emergency or to family members as authorized or required under other provisions of the medical records statute.

KP:cs