

1.1 A bill for an act

1.2 relating to data practices; enhancing certain penalties and procedures related to
1.3 unauthorized access to data by a public employee; amending Minnesota Statutes
1.4 2012, sections 13.04, subdivision 3; 13.05, subdivision 5; 13.055; 13.09.

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

1.6 Section 1. Minnesota Statutes 2012, section 13.04, subdivision 3, is amended to read:

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

1.19 (b) Notwithstanding section 13.15 or 13.43, or other law to the contrary, upon request,
1.20 to the extent the data are maintained by the government entity, an individual has access to
1.21 the name of persons who have obtained access to private data on the individual, unless the
1.22 data would identify an undercover law enforcement officer or are active investigative data.

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

2.4 Sec. 2. Minnesota Statutes 2012, section 13.05, subdivision 5, is amended to read:

2.5 Subd. 5. **Data protection.** (a) The responsible authority shall:

2.6 (1) establish procedures to assure that all data on individuals is accurate, complete,
2.7 and current for the purposes for which it was collected; and

2.8 (2) establish appropriate security safeguards for all records containing data on
2.9 individuals, including procedures for ensuring that data that are not public are only
2.10 accessible to persons whose work assignment reasonably requires access to the data, and
2.11 is only being accessed by those persons for purposes described in the procedure; and

2.12 (3) develop a policy incorporating these procedures, which may include a model
2.13 policy governing access to the data if sharing of the data with other government entities is
2.14 authorized by law.

2.15 (b) When not public data is being disposed of, the data must be destroyed in a way
2.16 that prevents its contents from being determined.

2.17 Sec. 3. Minnesota Statutes 2012, section 13.055, is amended to read:

2.18 **13.055 STATE AGENCIES; DISCLOSURE OF BREACH IN SECURITY;**
2.19 **NOTIFICATION AND INVESTIGATION REPORT REQUIRED.**

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

2.22 (a) "Breach of the security of the data" means unauthorized acquisition of or access
2.23 to data maintained by a state agency government entity that compromises the security and
2.24 classification of the data. Good faith acquisition of or access to government data by an
2.25 employee, contractor, or agent of a state agency government entity for the purposes of
2.26 the state agency entity is not a breach of the security of the data, if the government data
2.27 is not provided to or viewable by an unauthorized person, or accessed for a purpose not
2.28 described in the procedures required by section 13.05, subdivision 5. For purposes of this
2.29 paragraph, data maintained by a government entity includes data maintained by a person
2.30 under a contract with the government entity that provides for the acquisition of or access
2.31 to the data by an employee, contractor, or agent of the government entity.

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

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

3.4 (d) "Unauthorized person" means any person who accesses government data ~~without~~
3.5 ~~permission or~~ without a work assignment that reasonably requires ~~the person to have~~
3.6 ~~access to the data,~~ or regardless of the person's work assignment, for a purpose not
3.7 described in the procedures required by section 13.05, subdivision 5.

3.8 Subd. 2. **Notice to individuals; investigation report.** (a) A state agency
3.9 government entity that collects, creates, receives, maintains, or disseminates private or
3.10 confidential data on individuals must disclose any breach of the security of the data
3.11 following discovery or notification of the breach. Written notification must be made to
3.12 any individual who is the subject of the data and whose private or confidential data was, or
3.13 is reasonably believed to have been, acquired by an unauthorized person and must inform
3.14 the individual that a report will be prepared under paragraph (b), how the individual may
3.15 obtain access to the report, and that the individual may request delivery of the report by
3.16 mail or e-mail. The disclosure must be made in the most expedient time possible and
3.17 without unreasonable delay, consistent with (1) the legitimate needs of a law enforcement
3.18 agency as provided in subdivision 3; or (2) any measures necessary to determine the scope
3.19 of the breach and restore the reasonable security of the data.

3.20 (b) Upon completion of an investigation into any breach in the security of data, the
3.21 responsible authority shall prepare a report on the facts and results of the investigation.
3.22 If the breach involves unauthorized access to or acquisition of data by an employee,
3.23 contractor, or agent of the government entity, the report must at a minimum include:

3.24 (1) a description of the data that were accessed or acquired;

3.25 (2) the number of individuals whose data was improperly accessed or acquired;

3.26 (3) if there has been final disposition of disciplinary action for purposes of section
3.27 13.43, the name of each employee determined to be responsible for the unauthorized
3.28 access or acquisition;

3.29 (4) the final disposition of any disciplinary action taken against each employee in
3.30 response; and

3.31 (5) if disciplinary action was determined to be unnecessary, the specific findings and
3.32 reasons for that determination.

3.33 The report must not include data that are not public under other law. The report is
3.34 public and must be posted on the government entity's Web site, if the government entity
3.35 maintains a Web site, and provided to an individual who received the notification under
3.36 paragraph (a) and requested delivery of the report. If the government entity does not

4.1 maintain a Web site, the report must be posted on the principal bulletin board of the
4.2 government entity, or if the government entity does not have a principal bulletin board, on
4.3 the door of its usual meeting room.

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

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

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

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

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

4.19 (i) e-mail notice if the ~~state agency~~ government entity has an e-mail address for
4.20 the affected individuals;

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

4.23 (iii) notification to major media outlets that reach the general public within the
4.24 government entity's jurisdiction.

4.25 Subd. 5. **Coordination with consumer reporting agencies.** If the ~~state agency~~
4.26 government entity discovers circumstances requiring notification under this section of
4.27 more than 1,000 individuals at one time, the ~~state agency~~ government entity must also
4.28 notify, without unreasonable delay, all consumer reporting agencies that compile and
4.29 maintain files on consumers on a nationwide basis, as defined in United States Code, title
4.30 15, section 1681a, of the timing, distribution, and content of the notices.

4.31 Subd. 6. **Security assessments.** At least annually, each government entity shall
4.32 conduct a comprehensive security assessment of any personal information maintained
4.33 by the government entity. For the purposes of this subdivision, personal information is
4.34 defined under section 325E.61, subdivision 1, paragraphs (e) and (f).

4.35 **EFFECTIVE DATE.** This section is effective August 1, 2014, and applies to
4.36 security breaches occurring on or after that date.

5.1 Sec. 4. Minnesota Statutes 2012, section 13.09, is amended to read:

5.2 **13.09 PENALTIES.**

5.3 (a) Any person who willfully violates the provisions of this chapter or any rules
5.4 adopted under this chapter or whose conduct constitutes the knowing unauthorized
5.5 acquisition of not public data, as defined in section 13.055, subdivision 1, is guilty of a
5.6 misdemeanor.

5.7 (b) Willful violation of this chapter by, including any action subject to a criminal
5.8 penalty under paragraph (a), by any public employee constitutes just cause for suspension
5.9 without pay or dismissal of the public employee.

5.10 **EFFECTIVE DATE.** This section is effective August 1, 2014, and applies to crimes
5.11 committed on or after that date.