13.05 DUTIES OF RESPONSIBLE AUTHORITY.

Subdivision 1. [Repealed, 2012 c 290 s 72]

Subd. 2. [Repealed, 2012 c 290 s 72]

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

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

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

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

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

(d) Private data may be used by and disseminated to any person or entity if the individual subject or subjects of the data have given their informed consent. Whether a data subject has given informed consent shall be determined by rules of the commissioner.

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

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

Subd. 4a. **Informed consent for insurance purposes.** Informed consent for insurance purposes must comply with this subdivision, unless otherwise prescribed by the HIPAA Standards for Privacy of Individually Identifiable Health Information, Code of Federal Regulations, title 45, section 164. Informed consent for insurance purposes is not considered to have been given by an individual subject of data by the signing of a statement authorizing a government entity to disclose information about the individual to an insurer or its authorized representative, unless the statement is:

(1) in plain language;

(2) dated;

(3) specific in designating the government entity the data subject is authorizing to disclose information about the data subject;

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

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

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

(7) specific as to its expiration date, which must be within a reasonable period of time, not to exceed one year.

Notwithstanding clause (7), in the case of authorizations given in connection with applications for life insurance or noncancelable or guaranteed renewable health insurance that is so identified, the expiration date must not exceed two years after the date of the policy. An authorization in connection with medical assistance under chapter 256B or MinnesotaCare under chapter 256L or for individualized education program health-related services provided by a school district under section 125A.21, subdivision 2, is valid during all terms of eligibility.

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

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

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

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

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

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

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

Subd. 8. [Repealed, 2012 c 290 s 72]

Subd. 9. **Intergovernmental access of data.** A responsible authority shall allow another responsible authority access to data classified as not public only when the access is authorized or required by statute or

federal law. An entity that supplies government data under this subdivision may require the requesting entity to pay the actual cost of supplying the data.

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

Subd. 11. **Privatization.** (a) If a government entity enters into a contract with a private person to perform any of its functions, all of the data created, collected, received, stored, used, maintained, or disseminated by the private person in performing those functions is subject to the requirements of this chapter and the private person must comply with those requirements as if it were a government entity. All contracts entered into by a government entity must include a notice that the requirements of this subdivision apply to the contract. Failure to include the notice in the contract does not invalidate the application of this subdivision. The remedies in section 13.08 apply to the private person under this subdivision.

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

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

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

History: *1974 c 479 s 2; 1975 c 401 s 2; 1976 c 239 s 3; 1976 c 283 s 6,7; 1978 c 790 s 3; 1979 c 328 s 8; 1981 c 311 s 7,39; 1Sp1981 c 4 art 1 s 7; 1982 c 545 s 24; 1984 c 436 s 6-9; 1986 c 444; 1987 c 351 s 3; 1992 c 569 s 3; 1994 c 618 art 1 s 3; 1999 c 227 s 22; 1999 c 250 art 1 s 42; 2000 c 468 s 6,7; 2002 c 277 s 1; 2002 c 374 art 10 s 1; 2005 c 163 s 15-20; 2006 c 233 s 1; 2007 c 129 s 6; 2010 c 365 art 1 s 1,2; 1Sp2011 c 11 art 3 s 12; 2014 c 284 s 1; 2014 c 293 s 2*