MINNESOTA
BOARD OF COSMETOLOGY

Data Practices Policy: Employee Access to Not Public Data

This policy is required by Minnesota Statutes, sections 13.05, subdivision 5, and was adopted by the Minnesota Board of Cosmetology on October 16, 2017. The intent of this policy is to establish procedures ensuring appropriate access to not public data and provide a data inventory; this document is not intended to provide specific or general legal advice.

1000 University Avenue W, Suite 100
Saint Paul, MN 55104
651-201-2742
cosmetology@state.mn.us
mn.gov/boards/cosmetology

Legal Requirement

The Government Data Practices Act (Minnesota Statutes, Chapter 13) presumes that all government data are public unless a state or federal law says the data are not public. Government data means all recorded information a government entity has, including paper, email, flash drives, recordings, photographs, etc.

The law also says that the Board of Cosmetology must establish procedures ensuring appropriate access to not public data. This policy satisfies that requirement in Minnesota Statutes, section 13.05, subd. 5. By incorporating employee access to not public data in the board's data inventory (required by Minnesota Statutes, section 13.025, subd. 1) and in the individual employee's position description and procedures, this policy aims to limit access of not public data to employees whose work assignments reasonably require access.

Appropriate Access to Not Public Data

Any access to not public data will be strictly limited to the data necessary to complete an employee's work assignment. In the event of a temporary duty as assigned by a manager or supervisor, an employee may access certain not public data for as long as the work is assigned to the employee.

Tasks may be assigned by division, employee, or job classification. In the case of not public data that not all employees have a work assignment allowing access, the board will ensure that the not public data are secured electronically or physically. This policy also applies to employees who share workspaces where not public data are maintained.

The following measures limit inappropriate access to not public data:

- Employees are explicitly prohibited from intentionally accessing not public data that is not necessary to a work assignment.
- Employee position descriptions may contain provisions or indicators identifying any not public data accessible to the employee when a work assignment reasonably requires access.
- The board maintains assigned and appropriate security roles, limited access to appropriate shared network drives and licensing database, and password protected not public electronic data.
- All employee computers are password protected and locked before an employee leaves a workstation.
- Secured not public data are held within locked work spaces and in locked file cabinets.
- Not public documents are shredded before disposal.
- Employees are educated on data privacy and Minnesota Data Practices Act.
- The board maintains and adheres to a records retention policy.

Penalties for Unlawfully Accessing Not Public Data

The Board of Cosmetology will utilize the penalties for unlawful access to not public data as provided for in Minnesota Statutes, section 13.09, if necessary. Penalties include suspension, dismissal, or referring the matter to the appropriate prosecutorial authority who may pursue a criminal misdemeanor charge.

Data Sharing with Authorized Entities or Individuals

State or federal law may authorize the sharing of not public data in specific circumstances. Not public data may be shared with another entity if a federal or state law allows or mandates it. Individuals will have notice of any sharing in applicable Tennessen warnings (Minn. Stat. 13.04) or the board will obtain the individual's informed consent. Any sharing of not public data will be strictly limited to the data necessary or required to comply with the applicable law.

The board may make any data which is classified as private or confidential accessible to an appropriate person or agency if it determines that failure to do so is likely to create a clear and present danger to public health or safety (Minn. Stat. 13.41, subd. 6).

Inventory of Not Public Data

Minnesota Statutes Section 13.025, subd. 1, requires all state agencies to maintain an inventory of not public data that is retained by the agency. The board has prepared the following data inventory which identifies and describes not public data on individuals maintained by the board as of September 2017. This data inventory also includes the categorization of employees who may have access to not public data. In addition to the employees listed in the data inventory, the board's Responsible Authority, Data Practices Compliance Official, and Leadership Team may have access to all not public data maintained, if necessary for specified duties.

Name of Record, File, Process, or Data Type	Description	Data Classification and Citation	Employee Work Access
Social Security Numbers	Licensee and applicant social security numbers.	Private (Minn. Stat. 13.355)	Licensing, compliance, and inspections staff have access to this data for data entry and identification purposes.
Applicant for licensure data	Application data on current & former applicants for licensure collected to evaluate qualifications for licensure. Data includes name, designated address, education information, work history, previous license information, and other data. Name and designated address are public; all other data are private.	Private and Public (Minn. Stat. 13.41, subd. 2)	Licensing, compliance, and inspections staff whose work assignment requires access.
Complaint data – inactive and unsubstantiated	A. The identity of complainants who have made reports concerning licensees or applicants which appear in inactive complaint data are considered private, unless the complainant consents to the disclosure. B. The nature of unsubstantiated complaints when the information is not maintained in anticipation of legal action.	Private and public (Minn. Stat. 13.41)	Compliance, licensing, and inspections staff whose work assignment requires access may have access to this data.

	C. Inactive investigative data relating to violations of statutes or rules. D. The record of any disciplinary proceeding except data described in Minn. Stat. 13.41, subd. 5., which classifies the following as public data: orders for hearing, findings of fact, and conclusions of law and specification of the final disciplinary action contained in the record of the disciplinary action.		
Complaint data – active investigative data	Active investigative data relating to the investigation of complaints against any licensee.	Confidential (Minn. Stat. 13.41, subd. 4)	Compliance, licensing, and inspections staff whose work assignment requires access may have access to this data.
Personal contact information of subscribers	Telephone number and email address collected, maintained, or received from the public by a government entity for notification purposes or as part of a subscription list for an entity's electronic periodic publications as requested by the individual. Rulemaking email list not included.	Private (Minn. Stat. 13.356)	Select administrative staff may have access to this data to execute notifications and maintain the subscription service.
Attorney data	Data related to attorney work product or data protected by attorney-client privilege.	Private (Minn. Stat. 13.393)	Only the attorneys and necessary employees who will not, by seeing the data, destroy the privilege may see attorney-client privileged data.
Non-public data located in documents within scope of data requests	Data collected by data practices compliance official in responding to requests for data maintained by the board can include data that is itself already private under various laws. Staff working on responses must see this data in the course of fulfilling the request.	Private (Various)	Employees engaged in responding to the request may see all parts of that data.
Employee expense reports	Expense reimbursement requests submitted by employees who seek reimbursement for work-related expenses. Personal contact information is included on the report and considered private; all actual expense reimbursement data is public.	Public and Private (Minn. Stat. 13.43)	Administrative staff may see the private portion of this data, as may the submitting employee and the person authorizing and approving the report.
Personnel data	Data about employees and applicants, other than that defined as public in Minn. Stat. 13.43; labor relations information.	Private and confidential (Minn. Stat. 13.43)	Managers and supervisors may have access to this type of data for their specific staff, as necessary. Select administrative staff may have

			access for necessary administrative functions.
Continuity of Operations data	Personal home contact information used to ensure that an employee can be reached in the event of an emergency or other disruption affecting continuity of operation of a government entity.	Private (Minn. Stat. 13.43, subd. 17)	Senior leadership staff and select administrative staff may have access to COOP data.

Resources

Data Practices Contacts

Responsible Authority

Gina Fast, Executive Director

Phone: 651-201-2744

Email: Gina.Fast@state.mn.us

Data Practices Compliance Official

Catrina Mairose, Chief of Staff

Phone: 612-548-2176

Email: Catrina.Mairose@state.mn.us

Data Practices Designee

Jenna Bohl, Licensing Division Manager

Phone: 651-201-2750

Email: Jenna.Bohl@state.mn.us

Data Practices Office, Laws, and Rules

Minnesota Department of Administration – Data Practices Office
https://mn.gov/admin/data-practices/

Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13
www.revisor.leg.state.mn.us/statutes/?id=13

Data Practices Rules, Minnesota Rules Chapter 1205
www.revisor.leg.state.mn.us/rules/?id=1205

Data Practices Glossary

Courtesy of the Minnesota Data Practices Office and available at mn.gov/admin/data-practices/.

Classification of data: Determination by the Minnesota Legislature on whether government data are public or not public, whether the data subject gets access, and what additional rights flow to the data subject.

Confidential data: Government data about a person that are not available to the person or the public.

Data practices: The rules, regulations, and practices of Minnesota government in its handling of government data.

Data Practices Act (Chapter 13): The Minnesota law regulating how government handles data it collects, creates, maintains.

Data practices compliance official: Person in a government entity who handles data practices issues.

Data subject: The person or business/organization that government data are about.

Designee: A person the responsible authority designates to be in charge of certain records and to handle requests for government data.

Government entity: A unit of government, such as a state agency, city, county, school district.

Minnesota Rules, Chapter 1205: The Minnesota rules that relate and apply to Chapter 13.

Nonpublic data: Government data about businesses/organizations/inanimate objects that are available to the businesses/organizations but not to the public.

Not-public data: Any type of government data that are not available to the public – private, confidential, nonpublic, protected nonpublic. Government data: Everything government creates, collects, maintains that is recorded in some type of format.

Official record: Government data that document a government entity's official activities.

Public data: Government data that are available to anyone for any reason.

Private data: Government data about a person that are available to the person but not to the public.

Protected nonpublic data: Government data about businesses/organizations/inanimate objects that are not available to the businesses/organizations or the public.

Records retention schedule: A document that lists categories of official records and prescribes the length of time a government entity must keep its official records. Each government entity must have its own schedule or follow a general schedule.

Responsible authority: Person in a government entity who ultimately is responsible for matters relating to the Data Practices Act.

Tennessen warning notice: Specific information government must give a person when government collects data from that person. Named after the senate author of the original Data Practices Act – Bob Tennessen.