Minnesota Governor's Task Force on Broadband

July 21, 2016 Meeting

Minnesota government entity and contractor data security and breach notification

Melissa Krasnow

Minnesota Government Data Practices Act

Minnesota Director Data Security Risk Oversight

Other State Laws

Recommendations

Minnesota Government Data Practices Act

Covered Governmental Entities

Minnesota Government Data Practices Act applies to certain governmental entities, including:

- **State agencies**
- **Statewide systems**
- **Political subdivisions**
- **Contractor to a government entity**

Example of Government Entity Contract Provision

The requirements of Minnesota Statutes § 13.05, subd. 11 apply to this contract. The CONTRACTOR and GOVERNMENT ENTITY must comply with the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13, as it applies to all data provided by GOVERNMENT ENTITY in accordance with this contract, and as it applies to all data, created, collected, received, stored, used, maintained or disseminated by the CONTRACTOR in accordance with this contract. The civil remedies of Minnesota Statute §13.08 apply to the release of the data referred to in this clause by either the CONTRACTOR or GOVERNMENT ENTITY. In the event the CONTRACTOR receives a request to release the data referred to in this clause, the CONTRACTOR must immediately notify GOVERNMENT ENTITY. GOVERNMENT ENTITY will give the CONTRACTOR instructions concerning the release of the data to the requesting party before the data is released.

Some Data Definitions

Confidential data on individuals: data made not public and inaccessible to the individual subject of the data

Data on individuals: all government data where an individual is or can be identified as the subject of that data, unless the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of an individual

Government data: all data collected, created, received, maintained or disseminated by any government entity regardless of physical form, storage media or conditions of use

Some Data Definitions (con't)

Personal information: an individual's first name or first initial and last name together with one or more of the following data elements (when the data element is not secured by a method of technology that makes electronic data unreadable or unusable or was secured and the means necessary for reading or using the data was also acquired):

- **Social Security number**
- **driver's license number or Minnesota identification card number**
- **account number or credit or debit card number, together with any required security code, access code, or password that would permit access to an individual's financial account**

Private data on individuals: data made by statute or federal law applicable to the data: (i) not public and (ii) accessible to the individual subject of those data

Data Security

- **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**
- **Develop a policy incorporating these procedures**
- **Destroy not public data in a way that prevents its contents from being determined when being disposed of**
- **Conduct a comprehensive security assessment of any personal information maintained by the government entity at least annually**

Breach Notification Definitions

Breach of the security of the data: unauthorized acquisition of data maintained by a government entity that compromises the security and classification of the data

Unauthorized acquisition: a person has obtained, accessed or viewed government data without the informed consent of the individuals who are the subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes

Written Breach Notification

Notification of a breach to:

- **any individual who is the subject of the data and whose private or confidential data was, or is reasonably believed to have been, acquired by an unauthorized person and inform the individual that: (1) a report will be prepared, (2) how the individual may obtain access to the report and (3) that the individual may request delivery of the report by mail or e-mail, in the most expedient time possible and without unreasonable delay**
- **all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices where there are more than 1,000 individuals to be notified at one time, without unreasonable delay**

See also slide 12, Minnesota Office of the Legislative Auditor

Breach Notification Investigation Report

Responsible authority must prepare a report on the facts and results of the investigation upon completion of an investigation into a breach

If the breach involves unauthorized access to or acquisition of data by an employee, contractor or agent of the government entity, the report must include, at a minimum:

- **a description of the type of data that were accessed or acquired**
- **the number of individuals whose data was improperly accessed or acquired**
- **if there has been final disposition of disciplinary action, the name of each employee determined to be responsible for the unauthorized access or acquisition**
- **the final disposition of any disciplinary action taken against each employee in response**

Minnesota Office of the Legislative Auditor

MN Legislature | Get Connected | About the Legislature | Mobile Site | Search Legislative Auditor

House | Senate | Joint | Schedules | Legislators | Committees | Bills | Law | Multimedia | Publications

Minnesota Office of the Legislative Auditor

OLA Financial Audit Division

About the OLA | Program Evaluation Division | Financial Audit Division | Special Reviews/Investigations

Report Summary
MNsure: An Unauthorized Disclosure of Private Data
Special Review

Financial Audit Division Report 13-27 — Released November 7, 2013

On September 12, 2013, a MNsure employee e-mailed a document with private data in it to an individual not authorized to see the data. The next day, the Office of the Legislative Auditor learned of the disclosure and initiated a special review. We reached two conclusions based on the following findings:

Conclusions and Findings

The disclosure by a MNsure employee was unintentional; we found no evidence of malicious intent. MNsure responded appropriately after the disclosure occurred.[1]

- The unauthorized disclosure of private data occurred when a MNsure employee mistakenly attached a document containing private data to an e-mail. We found no evidence of malicious intent.
- MNsure responded quickly to the unauthorized exposure of private data and followed the notice requirements of state law.

In developing a certification process for insurance brokers, MNsure officials made decisions that contributed directly to the disclosure of private data.

- MNsure decided to collect Social Security numbers from insurance brokers although that data was not needed for MNsure to fulfill its responsibilities.
- MNsure decided to collect personal data, including Social Security numbers, from insurance brokers using e-mail without fully assessing and mitigating the risks involved and without considering a more secure and efficient alternative.
- MNsure did not adequately secure private data residing on its internal computer network.
- MNsure assigned few staff to develop the broker certification process.
- MNsure did not effectively organize the information it collected from brokers.
- MNsure relied on data security and privacy training that may not have been adequate.

[1] Our conclusion does not include a judgment on MNsure's decision to terminate the employee who disclosed private data.

More Information

Full Report (PDF)

Manager: Jim Nobles

MORE INFORMATION

Map and Directions
Website Policies

REPORT WRONGDOING

Report Possible Misuse of Public Money or Other Resources

CONTACT US

Phone: (651) 296-4708
Fax: (651) 296-4712
TTY/TDD Relay: (800) 627-3529
E-Mail: Legislative.Auditor@state.mn.us
Hours: 8:00 A.M. - 4:30 P.M.
Map and Directions

GET CONNECTED

Sign-up for Report Release Notifications

Office of the Legislative Auditor • Room 140, 658 Cedar St., St. Paul, MN 55155

Remedies and Penalties

- **Action for damages**
- **Injunction**
- **Action to compel compliance**
- **Criminal penalty where willful violation or knowing unauthorized acquisition of not public data**

Minnesota Director
Data Security Risk Oversight

Minnesota Business Corporations

A director shall discharge the duties of the position of director in good faith, in a manner the director reasonably believes to be in the best interests of the corporation, and with the care an ordinarily prudent person in a like position would exercise under similar circumstances. A person who so performs those duties is not liable by reason of being or having been a director of the corporation.

Good faith means "honesty in fact in the conduct of the act or transaction concerned."

Minnesota D&O Litigation: Target Shareholder Derivative Lawsuit

- **Target's board appointed a Special Litigation Committee which determined it was not in Target's best interests to pursue the derivative claims**
- **Special Litigation Committee's motion for approval and dismissal and Defendants' motions to dismiss were granted via order on July 7, 2016**
- **Notice of order must be furnished in a Form 8-K to the SEC and provided by electronic mail to counsel for the shareholder who made demand on Target's board**
- **If no shareholder seeks to intervene within 30 days of Target furnishing notice of order to the SEC, this matter will be dismissed with prejudice**

Other State Laws

Other State Laws

- **Other states have laws that differ from the Minnesota Government Data Practices Act**
- **Other state laws cover specific areas such as open records/public records, data security or breach notification**

See http://www.house.leg.state.mn.us/hrd/issinfo/datacommission_overview2014.pdf

State Data Security Laws

- **12 states have laws addressing security procedures that apply to businesses**
- **Minnesota does not have a data security law that applies to businesses**
- **Some state data security laws apply to both businesses and government entities (for example, Illinois)**
- **Other state data security laws apply to businesses only (for example, California)**

State Breach Notification Laws

- **47 states, plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands, have breach notification laws for businesses (including separate Minnesota breach notification law, Minn. Stat. § 325E.61, for businesses)**
- **Alabama, New Mexico and South Dakota do not have breach notification laws**
- **Some state breach notification laws apply to both businesses and government entities (for example, Illinois)**
- **There are separate state breach notification laws for businesses and government entities in other states (for example, California)**

Minnesota Data Security and Breach Notification Laws

Data security:

- **Minnesota Government Data Practices Act applies to government entities and their contractors**

Breach notification:

- **Minnesota Government Data Practices Act applies to government entities and their contractors**
- **Minn. Stat. § 325E.61 applies to businesses**

Recommendations

Recommendations – Privacy Laws and Developments

- **Government entities and their contractors should determine which laws apply to them**
- **State privacy laws continue to change, as do federal privacy laws; note developments, including cyber attacks and litigation**
- **Monitor these changes and developments - approaches**
- **Take governance into account**

Recommendations – Contracts; Incident Response Plans; Training; Insurance

- **Inventory and maintain contracts so they are readily available; review privacy provisions**
- **Implement and update incident response plan; testing: tabletop exercises (TTXs)**

See https://www.irmi.com/articles/expert-commentary/guidance-for-incident-response-plans

- **Conduct training and awareness**
- **Consider cyber liability insurance**