

## S.F. No. 1606 – Insurance Data Security Law

**Author:** Senator Paul J. Utko

**Prepared by:** Christopher B. Stang, Senate Counsel (651/296-0539)

**Date:** March 5, 2021

---

This bill is intended to adopt the NAIC Insurance Data Security Model Law for Minnesota.

**Section 1** establishes definitions for purposes of the act.

**Section 2, subd. 1** requires insurers to develop, implement, and maintain comprehensive written information security program based on its risk assessment.

**Subd. 2** sets forth objectives of the security program.

**Subd. 3** requires the insurer to designate a responsible party who is responsible for the program. Requires licensees to conduct a risk assessment.

**Subd. 4** requires the licensee to design its information security program in light of its risk assessment. Must determine which of listed security measures are appropriate and implement them.

**Subd. 5** requires the board of directors to maintain oversight of the information security program.

**Subd. 6** requires due diligence in selecting its third-party service provider.

**Subd. 7** requires adjustment of the security program consistent with ongoing risk assessment.

**Subd. 8** requires licensees to establish a written incident response plan. the plan must address specified areas.

**Subd. 9** requires an annual certificate of compliance be submitted to the commissioner.

**Section 3** requires a prompt investigation if a cybersecurity event occurs. Scope of the investigation specified. Records must be retained for at least five years from date of cybersecurity event.

**Section 4** requires the licensee to notify the licensing commissioner within three business days of a cybersecurity event under specified circumstances. Licensee must provide as much of listed information as possible. Notice to consumers required if the consumer's nonpublic information was or is reasonably believed to have been acquired by an unauthorized person. Notice must be provided by one of the listed methods. Notification requirements when system maintained by third party or licensee acting as a reinsurer set forth, and when the insurer must provide notice to the producer of record.

**Section 5** gives the licensing commissioner power to investigate conduct that may be in violation of the act.

**Section 6** makes specified documents and materials confidential. Information is not subject to subpoena or discoverable. Commissioner may share information with other regulatory agencies.

**Section 7** exempts certain licensees from the act, including those with fewer than 25 employees and licensees subject to HIPAA.

**Section 8** cross references enforcement options for violations.

**Section 9** repeals statutes obsolete upon enactment of this act.

**Section 10** provides for effective dates. Implementation schedule specified.