Insurance Data Security Model Law (#668)
FAQs

1. What accounts for slight differences in the confidentiality provisions in certain NAIC model laws?
   - More than a dozen NAIC model laws generally follow a confidentiality template developed in 1999. The *Insurance Data Security Model Law* (#668) and other NAIC model laws like the *Risk Management and Own Risk Solvency Assessment Model Act* (#505) (ORSA) or the *Insurance Holding Company System Regulatory Act* (#440) (Holding Company) generally follow the NAIC confidentiality template. Where differences in confidentiality language exist, the language is tailored to the type of confidential information being protected and the manner in which the regulator is authorized to share confidential information.

2. What is the nature of the information provided to state insurance regulators under the ORSA and Holding Company model laws?
   - The ORSA and Holding Company model laws can involve the disclosure to the regulator of forward-looking business plans and commercially-sensitive proprietary information dealing with how companies manage internal processes. Such information may be included in the Enterprise Risk Report (or Form F) under the Holding Company law and the ORSA Summary Report under the ORSA law. Information of this nature, if disclosed inappropriately, could put a company at a competitive disadvantage and thus requires enhanced confidentiality protections. This information is not the type of information provided to the regulator under Model #668.

3. Why does the *Insurance Data Security Model Law* (#668) not characterize information that may be disclosed to the commissioner as proprietary and trade secret information similar to the ORSA law?
   - The factual information about the occurrence of a cybersecurity event provided to the commissioner is not a trade secret. Therefore, Model #668 does not automatically classify such information as proprietary and trade secret information. Model #668 classifies several categories of information as confidential and provides protections from disclosure based on the NAIC confidentiality template. Model #668 does not preclude an insurer from seeking trade secret protection under state trade secret law, if warranted.

4. Why does Model #668 not prohibit the commissioner from disclosing certain information without the consent of the insurer as the ORSA law does?
   - Both model laws include strong confidentiality protections for certain categories of information disclosed to the commissioner under each model law. The ORSA model law does not involve personal consumer information. Because the personal information breached in a cybersecurity event directly impacts consumers and Model #668 provides the commissioner discretion to fulfill his or her duty to protect consumers and their data, the commissioner is not barred from using his or her judgment to disclose information as necessary. Disclosure is not required; rather, the commissioner maintains their authority to disclose information that may be needed to inform consumers about a data breach without seeking a company's consent.

5. How is the confidentiality of this information maintained during litigation?
   - Information in the control or possession of the Department is confidential and privileged by law under Model #668 and the ORSA and Holding Company model laws. However, these protections do not render this information exempt from a subpoena or discovery request made directly to an insurer. Furthermore, in the event the commissioner is conducting an investigation or examination under the state examination law, the confidentiality protections of that law would also apply. Put another way, the confidentiality provisions are directed at protecting from disclosure information in the possession or control of the commissioner or anyone acting under his or her authority.