Data Privacy and Security Requirements for the Insurance Sector

Presented to the Insurance Consumer Affairs Exchange

Jennifer McAdam, NAIC Senior Counsel

November 17, 2021

NAIC NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Data Privacy vs. Data Security

Data Privacy

- How data is collected & used
- Procedures & policies governing collection and appropriate use of personal data
- Consumers retain control over how their personal data is used
- Ex: California Consumer Privacy Act (CCPA)

Data Security

- How data is stored & protected: security measures & safeguards
- Procedures & policies to ensure data isn't being used or accessed by unauthorized parties
- Ex: *Insurance Data Security Model Law*

NAIC Data Security Model Laws

Standards for Safeguarding Customer Information Model Regulation (#673)

- Adopted in 2002
- Based on:
  - Gramm-Leach-Bliley Act (GLBA)
  - Federal Financial Industry Regulators' GLBA Regulations

Insurance Data Security Model Law (#668)

- Adopted in 2017
- Based on:
  - Gramm-Leach-Bliley Act (GLBA)
  - NY DFS Cybersecurity Requirements for Financial Services Companies

NAIC Data Privacy Model Laws

NAIC Insurance Information and Privacy Protection Model Act (#670)

- Adopted in 1980
- Based on:
  - Fair Credit Reporting Act (FCRA)
  - Federal Privacy Act (FPA)

Privacy of Consumer Financial and Health Information Regulation (#672)

- Adopted in 2000
- Based on:
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA)

Model #670 Key Provisions

- Sets standards for the collection, use, and disclosure of information gathered in connection with insurance transactions.
- Requires insurers to provide notice that alerts the individual of the insurer's information practices.
- Gives consumers right to their personal information.

Model #670 Key Provisions (cont.)

Gives consumers right to request an insurer:

- Provide access to recorded personal information;
- Disclose the identity of the third parties to whom the insurance disclosed the information;
- Provide the source of the collected information;
- Correct and amend the collected information; and
- Delete the collected personal information.

Model #672 Key Provisions

- Requires insurers provide notice to consumers about privacy policies and practices;
- Describes the conditions under which an insurer may disclose nonpublic personal health information and nonpublic personal financial information about individuals to affiliates and nonaffiliated third parties; and
- Provides methods for individuals to prevent an insurer from disclosing that information:
  - "opt out" for financial info and "opt in" for health info.
- Enforced via the state's Unfair Trade Practices Act.

State Adoption of Privacy Models

- *NAIC Insurance Information and Privacy Protection Model Act* (#670)
  - ➢17 states
- *Privacy of Consumer Financial and Health Information Regulation* (#672)
  - ➢Every state has a version (19 have adopted only financial requirements – not health)

Privacy Standards in Market Conduct Examinations

- **Standard 10:** Procedures for the collection, use and disclosure of information gathered in connection with insurance transactions.
- **Standard 11:** Develop and implement written policies, standards and procedures for the management of insurance information.
- **Standard 12:** Policies and procedures to protect the privacy of nonpublic personal information.
- **Standard 13:** Provide privacy notices to customers and consumers regarding treatment of nonpublic personal financial information.

Privacy Standards in Market Conduct Examinations

- **Standard 14:** Policies and procedures so that nonpublic personal financial information will not be disclosed when a consumer has opted out and the regulated entity provides opt-out notices to its customers and consumers.
- **Standard 15:** Collection, use and disclosure of nonpublic personal financial information are in compliance with applicable statutes, rules and regulations.
- **Standard 16:** In states with the health information provisions of Model #672, the entity has policies and procedures in place so that nonpublic personal health information will not be disclosed, unless the customer or consumer has authorized the disclosure.

State Comprehensive Data Privacy Laws

1. California Consumer Privacy Act (CCPA) &
   California Privacy Rights Act (CPRA)

2. Colorado Privacy Act (CPA)

3. Virginia Consumer Data Protection Act (CDPA)

State Comprehensive Data Privacy Laws

Privacy Law	Disclose Collected Info	Disclose Sources of info	Disclose Business Purpose	Disclose 3rd-Party Involved	Right to Delete Info.	Portable Format	Right to Correct Info.	Right to Restrict Use	Opt-Out / Opt-In	Private Right of Action	Enforced by AG	Anti-Discrimination	HIPAA Exempt.	GLBA Exempt.
CA - CCPA & CPRA	X	X	X	X	X	X			Out	X	X	X	X	X
CO - CPA	X		X		X	X	X		Out		X		X	X
VA - CDPA	X		X	X	X	X	X		Out		X	X	X	X

NAIC Privacy Protections Working Group

2021 Charges

- Review state insurance privacy protections regarding the collection, use and disclosure of information gathered in connection with insurance transactions, and make recommended changes, as needed, to certain NAIC models, such as the *NAIC Insurance Information and Privacy Protection Model Act* (#670) and the *Privacy of Consumer Financial and Health Information Regulation* (#672).

https://content.naic.org/cmte_d_ppwg.htm

Jennifer McAdam
NAIC
Senior Counsel
816.783.8878
jmcadam@naic.org