Data Privacy Law Overview

Privacy Protections (D) Working Group

Jennifer McAdam
Senior Counsel

DECEMBER 8, 2019

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

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 Privacy Model Laws

- **1980:** *NAIC Insurance Information and Privacy Protection Model Act* (#670)
- **1998:** *Health Information Privacy Model Act* (#55)
- **2000:** *Privacy of Consumer Financial and Health Information Regulation* (#672)

Model #670 Legislative History

- **1970:** Fair Credit Reporting Act
  - Addresses the fairness, accuracy and privacy of the personal information contained in the files of the consumer reporting agencies.
- **1974:** Federal Privacy Act
  - Governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

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 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;
  - Amend the personal information; and
  - Delete the collected personal information.

Model #670 Key Definition

"Personal information" means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health or any other personal characteristics.

Includes an individual's name and address and "medical record information" but does not include "privileged information".

Model #55 Key Provisions

Requires carriers to:

- Create policies, standards and procedures governing health information
- Notice of policies, standards and procedures
- Consumer right to access PHI
- Consumer right to amend PHI
- Provide list of disclosures of PHI
- Obtain authorization for collection, use or disclosure of PHI (with exceptions)

Model #55 Key Definitions

Health information: any information or data, whether oral or recorded in any form or medium, and personal facts or information about events or relationships that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual or a member of the individual's family;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Protected health information (PHI): health information:

(1) That identifies an individual who is the subject of the information; or

(2) With respect to which there is a reasonable basis to believe that the information could be used to identify an individual.

Model #672 Legislative History

- Provisions governing protection of health information based on:
  - *Health Information Privacy Model Act* (#55); and
  - HHS health information privacy regulations (pursuant to HIPAA)
- Provisions governing protection of financial information are based on privacy regulations promulgated by federal banking agencies.

Model #672 Key Provisions

- Requires insurers provide notice to consumers about its privacy policies and practices;
- Describes the conditions under which a licensee 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 a licensee from disclosing that information:
  - "opt out" for financial info and "opt in" for health info.
- Enforced via the state's Unfair Trade Practices Act.

Model #672 Key Definitions

Health information: any information or data except age or gender, whether oral or recorded in any form or medium, created by or derived from a health care provider or the consumer that relates to:

(1) The past, present or future physical, mental or behavioral health or condition of an individual;

(2) The provision of health care to an individual; or

(3) Payment for the provision of health care to an individual.

Personally identifiable financial information: any information:

(1) A consumer provides to a licensee to obtain an insurance product or service from the licensee;

(2) About a consumer resulting from a transaction involving an insurance product or service between a licensee and a consumer; or

(3) The licensee otherwise obtains about a consumer in connection with providing an insurance product or service to that consumer.

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 to minimize any improper intrusion into the privacy of applicants and policyholders.
- **Standard 11:** Developed and implemented written policies, standards and procedures for the management of insurance information.
- **Standard 12:** Policies and procedures to protect the privacy of nonpublic personal information relating to its customers, former customers and consumers that are not customers.
- **Standard 13:** Provides privacy notices to its customers and, if applicable, to its consumers who are not customers regarding treatment of nonpublic personal financial information.

Privacy Standards in Market Conduct Examinations cont.

- **Standard 14:** If the regulated entity discloses information subject to an opt-out right, the regulated entity has policies and procedures in place so that nonpublic personal financial information will not be disclosed when a consumer who is not a customer has opted out, and the regulated entity provides opt-out notices to its customers and other affected 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 promulgating the health information provisions of Model #672), or providing equivalent protection through other substantially similar laws, entity has policies and procedures in place so that nonpublic personal health information will not be disclosed, except as permitted by law, unless a customer or a consumer who is not a customer has authorized the disclosure.

General Data Protection Regulation (GDPR)

- Effective May 2018
- Applies to U.S. companies that collect data from citizens of the EU over the internet
- Requires companies to obtain explicit consent from consumers to collect their data (“opt in”) with an explanation of how the data will be used (consent can be withdrawn anytime)
- Provides standards for safeguarding the data

California Consumer Privacy Act (CCPA)

- Effective January 1, 2020
- Applies to for-profit companies that do any business in California
- First U.S. “omnibus” privacy law – imposes broad obligations on businesses to provide consumers with transparency and control of their personal data

California Consumer Privacy Act (CCPA)

Consumer has right to request that a business:

- Disclose:
  - categories and specific pieces of personal information collected;
  - categories of sources the information was collected from; business purpose for collecting the information; and
  - categories of third parties with whom the information is shared, and the specific pieces of personal information that was shared
- Delete any personal information;
- Right to opt-out of information being disclosed to third parties. With separate opt-in requirements for minors.
- Right not be discriminated against for exercising rights (nondiscrimination provision)

CCPA Exemptions

- Full exemption for protected health information governed by HIPAA and a partial exemption for information subject to GLBA.

- If the information subject to GLBA is breached, the consumer can pursue a private civil action against the company.

CCPA Key Definition

Personal Information: Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household such as a real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers

State Data Privacy Legislation

- 24 states introduced data privacy legislation but only three passed: Illinois, Maine and Nevada.
  - Illinois: law bans insurers from using genetic testing information to set health or accident rates.
  - Maine: law bans internet providers from selling personal information without consent.
  - Nevada: law requires businesses to allow consumers to opt out of any sale of their personal information. There are exemptions for entities subject to GLBA and HIPAA.
- Five states passed bills establishing task forces to study the issue of data privacy by reviewing laws in other states and making recommendations.
  - Connecticut, Hawaii, Louisiana, North Dakota, and Texas.
- Uniform Law Commission established the Collection and Use of Personally Identifiable Data Committee

Comparison: CCPA and Model #670

CCPA

Consumer right to request that a business:

- Disclose the categories and specific pieces of personal information collected;
- Disclose categories of sources;
- Disclose business purpose for collecting the information;
- Disclose categories of third parties with whom the information is shared, and specific pieces of personal information shared;
- Right to access, correct, delete.

Model #670

Individual right to request that an insurer:

- Disclose types of personal information collected;
- Disclose sources of the collected information;
- Disclose purpose for collecting the information
- Disclose identity of the third parties to whom information is disclosed;
- Right to access, correct, delete.

Considerations

- What types of data collection, sharing, and usage are specific to insurers?
- What are privacy risks that affect insurance consumers?
- Where are gaps in federal and state law?
- What obligations should insurers have to consumers?
- What rights should consumers have to control their personal information?

Jennifer McAdam
NAIC
Senior Counsel
816.783.8878
jmcadam@naic.org