08/27/21

PRINCIPLES FOR CONSUMER DATA PRIVACY IN INSURANCE

Harold M. Ting, PhD
NAIC Consumer Representative

Just as the Declaration of Independence laid out truths that our country's founders felt were self-evident, I feel the principles below are self-evident guarantees that Privacy Protection Work Group members should consider when discussing consumer privacy. These principles may help to resolve differences in opinion, because they are based on fundamental values that I hope we all share.

1. Only insurance-related businesses that need unpublished, personal consumer data to complete insurance transactions should be allowed to collect such data. Lead generating companies that only collect such data to sell it to other businesses do not meet this criterion. Insurers that get leads from companies that solicit quotes for consumers should only contract with companies that agree not to sell or share consumer data they collect.

2. Such businesses should only collect data that is essential for transactions. Collecting other data is not justified.

3. Insurers and related parties should only keep such data as long as it is needed for the transaction or to meet regulatory requirements. When that data is not needed anymore, it should be deleted.

4. Businesses should not transfer or sell this data to other business entities, whether they are related or not, if such transfer or sale is not essential for the insurance transaction that a consumer seeks. If a consumer wants information about services or products that s/he did not request, it should only be the consumer's choice whether to be contacted. If a business wishes to recommend services or products of other business entities, then it should ask the consumer if s/he would like such information.

5. Insurers should share all data with a consumer that have a material impact on the consumer's purchase or receipt of services, so the consumer can verify whether the data used is correct. Errors in data occur when it is out-of-date, is misreported by third parties, or where data entry mistakes have occurred. Insurers can develop a standard data set format for meeting this requirement to minimize the burden of meeting it.

6. If it is determined that a business has incorrect personal data, it is the responsibility of that business to correct that data and to ensure that other data collecting entities it used also correct that data. The business responsible for having corrections made should spot check periodically to make sure these corrections are being made by itself and other entities.

7. Insurers should never use information from consumer tracking programs that use cookies or other software tools to collect data on a consumer's online activities, even if the consumer permitted the use of such software on their electronic devices. It is not reasonable to assume that consumers will be aware of what is being collected and how it is being used.

8. Exceptions to these principles should only be allowed to meet HIPAA regulations or other legal requirements. In such cases, consumers should be notified when such exceptions occur and be informed what unpublished personal data was used and the reasons why.

9. It should be the responsibility of regulatory authorities to ensure that these requirements are met and to establish sufficient penalties to incent compliance. Consumers do not have the tools and expertise to investigate compliance on a case-by-case basis.