CARLTON FIELDS

Cast Into the Deep: Questions for Charting New Privacy Waters

May 05, 2021

As insurers consider new data from new sources and new means for consumer outreach, working through the privacy requirements is like navigating choppy waters. The various privacy regimes include:

- Gramm-Leach-Bliley Act (GLBA) and state equivalents that govern financial institutions' use, collection, and sharing of consumer information and require certain notices and consents based on the type of information collected, its use, and with whom it is shared.
- Fair Credit Reporting Act (FCRA) regarding the use of credit reports (broadly defined) and imposing requirements for notices, authorizations, and permitted uses.
- Health Insurance Portability and Accountability Act (HIPAA) governing the use of health information by covered entities and their business associates and requiring certain notices, authorizations, and cybersecurity precautions.
- Federal marketing laws, such as the Telephone Consumer Protection Act (TCPA), the Telemarketing Sales Rule (TSR), and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), that require certain notices, authorizations, and consents for certain consumer outreach.
- Driver Privacy Protection Act (DPPA) and state equivalents that govern the use and disclosure of information gathered by state departments of motor vehicles.
- State insurance laws requiring certain notices and authorizations and cybersecurity policies and procedures. State insurance laws vary widely but can require the provision of rights of access, modification, and deletion, and prohibit certain uses of information and business practices.

- State privacy laws requiring particular notices and consents, contractual provisions in partner relationships, reasonable cybersecurity measures, and additional rights (such as the right to know, correct, or delete certain information), and prohibiting certain practices. This is an area of especially rapid growth and, for insurers, often involves a close analysis of state laws' GLBA exemptions.
- Contractual obligations to third parties from whom you collect data.

These regimes include many different and overlapping requirements as to the notices you provide to, and the acknowledgments or authorizations you seek from, consumers. And their proper application requires careful consideration and analysis of their requirements and exceptions.

Here are seven questions for smooth sailing through the seven seas of privacy:

1. What data will be collected and from whom?
   Different privacy laws apply to different data, and different states define that data differently. So the first step is to make sure everyone on board understands key terms the same way. Next, take stock of the data that will be collected throughout the process, so you can evaluate potential laws implicated. Will you collect health data? Pull credit reports? Use DMV information?

   The same data may trigger different obligations depending on whose data is being collected. For example, a life insurer collecting health information from a consumer need not be concerned with HIPAA. Some state insurance laws, however, require a notice of health information practices and associated rights, as well as an authorization, if health data is collected from any source besides the consumer or is shared for certain purposes.

2. How will the data be used — only for servicing and administration or also for marketing?
   Some uses of consumer data are "givens" for which the consumer cannot opt out. Other uses, however, are not. For example, even if consumers cannot opt out of an insurer using their information to underwrite their policy, the insurer may need consent to use consumers' information for marketing purposes. Separately, consider the type of consent needed. While opt-out consents may be sufficient for some uses, opt-in consents are necessary for others. If you intend to use the information for marketing purposes, consider how you intend to do such outreach. Do you plan to text consumers? Email them? Call them? What technologies do you intend to use? A single authorization can be drafted to encompass all these forms of outreach, capturing the many obligations of the TCPA, TSR, and CAN-SPAM, as well as common contractual requirements imposed by these service providers.

3. Will the data be shared with others and for what purposes?
   How you will use or share the data you collect has a significant impact on what notices and consents you need. Your use of the data and with whom you share it is particularly important for determining your GLBA obligations, as many uses are exempt from the GLBA's requirements to provide notice and an opportunity to opt out. Also, sharing with affiliates versus nonaffiliates can have very different consequences. For example, depending on when you intend to share data with a nonaffiliate and for what purpose, you may not need to provide a consumer with your GLBA notice until the consumer becomes your customer.

   When designing your procedures, remember to consider not only your own statutory privacy obligations but also those you contractually inherit based on statutes that apply to your partners. For example, if you are contracting with a HIPAA-covered entity or business associate, you will likely inherit some HIPAA obligations.

   If you are sharing consumer information with any parties, remember to include the necessary restrictions and certifications in your contracts to prevent that sharing from being considered a "sale."

4. How will you document your compliance?
   Function under the maxim, "If you can't prove it, it didn't happen." Make sure your process creates a record of your compliance. Be aware of the evidence you are creating.

5. How close to the wind will you sail?
   Privacy is not the only consideration factoring into your decision-making, and business and legal factors need to be weighed. Privacy laws, moreover, are notoriously ambiguous and frequently develop so quickly that there is little interpretive guidance. Your ultimate approach will require a decision about how much risk of noncompliance is acceptable under the circumstances. Not all privacy law violations carry the same consequences.

6. How often do you want to revisit your process?
   Given the speed at which new privacy legislation is being passed, some insurers base their plans not only on currently enacted legislation but also on expected privacy trends and developments. This can help avoid being in a constant state of catch-up.

7. How will you protect the data you collect?
   Batten down the hatches. All data collection and retention brings with it a risk of a breach and its fallout. Prepare now to minimize your risk. Contract and insure appropriately.

Fair winds and following seas!

Authored By

Ann Young Black

Patricia M. Carreiro

Related Practices

Financial Services Regulatory
Cybersecurity and Privacy
Life, Annuity, and Retirement Solutions

Related Industries

Life, Annuity, and Retirement Solutions
Securities & Investment Companies
Life, Annuity, and Retirement Solutions