

CLIENT ALERT

California SB 354: A New Privacy Framework for the Insurance Industry

October 8, 2026

AUTHORS

Daniel K. Alvarez | Stephanie Duchene | Laura E. Jehl

In 2018, California led the charge on consumer privacy by enacting the California Consumer Privacy Act (“CCPA”), the first state-level comprehensive privacy law. Eight years later, California is again taking the lead on privacy, this time enacting sweeping changes to the state’s Insurance Information and Privacy Protection Act (“IIPPA”). Senate Bill 354 (“SB 354”), signed into law by Governor Newsom on September 27, 2026, establishes one of the most comprehensive insurance-specific privacy regimes in the United States. In particular, it moves California insurance privacy law away from the traditional notice-and-consent framework towards a broader regime governing how insurers and other covered entities collect, use, analyze, retain, share, secure, and ultimately delete personal information.

The changes enacted in SB 354 become operative on July 1, 2028. That gives covered entities approximately 21 months to implement changes to their privacy compliance efforts—time that most entities will need. For many covered entities, compliance with the revised IIPPA will require detailed data mapping, documentation and classification of processing purposes; implementation of a robust consumer-rights infrastructure, and changes to consent systems, retention schedules, and vendor contracts. In this client alert, we highlight some of the major changes enacted by SB 354 and their practical effects—both with respect to compliance issues specific to insurers in California and with respect to broader efforts to update insurance privacy laws across the U.S.

SB 354: More Companies and Data Covered, More Restrictions and Governance Required

SB 354 does not create insurance privacy regulation from scratch, but it does expand and reorganize the applicable requirements. That is particularly evident with respect to the scope of companies and data that are now subject to IIPPA as well as with respect to some of the new substantive requirements and restrictions.

On entity scope, SB 354 applies principally to “licensees”—defined broadly to include persons licensed, authorized, registered, or required to be licensed or registered under the Insurance Code, and expressly includes insurers and producers. Moreover, it directly imposes obligations on *third-party service providers* to the extent those providers process or share consumer personal information in connection with the business of insurance or engage in insurance transactions with consumers. This is a significant change. IIPPA and other legacy insurance privacy laws addressed vendor concerns indirectly, through the regulated insurer’s own disclosure and security obligations. In contrast, *SB 354 makes third-party compliance governance a central component of the statutory scheme.*

The expansion in data scope is potentially more significant. SB 354 replaces the traditional focus on information associated with an insurance transaction with a broader, CCPA-like definition of “personal information” that includes “information processed or shared in the business of insurance that identifies, relates to, describes, can reasonably be associated with, or can reasonably be linked—directly or indirectly—to a consumer or household.” The definition expressly encompasses identifiers, commercial information, protected classifications, biometrics and other categories. The bill separately creates a broad category of *sensitive personal information*, including government identifiers, precise geolocation, race and ethnicity, citizenship and immigration status, health information, and biometrics, among other data categories, to which more robust restrictions attach. Even for insurers that have always been subject to IIPPA, this expanded and more granular scope raises questions well beyond traditional policy and claims files, particularly as these companies increasingly use telematics, digital engagement data, external datasets, sophisticated underwriting models, AI systems, and behavioral or property information in their operations.

The most consequential substantive change is the introduction of a general principle that processing must be “reasonably necessary and proportionate” to the purpose for which the information was collected or another permitted or disclosed purpose. Insurance transactions, legal compliance, fraud-related functions and specified operational activities remain permissible, but SB 354 overlays those uses with data-minimization and purpose-limitation concepts familiar from modern comprehensive privacy laws.

Consistent with this addition, notice requirements are substantially more prescriptive. A covered entity generally must provide a clear and conspicuous, stand-alone privacy notice—with information and disclosures much more akin to a CCPA notice than a the traditional Gramm-Leach-Bliley Act (“GLBA”) notice more familiar to financial institutions—within 21 calendar days after first collecting, processing, or sharing personal information, and licensees must provide recurring privacy-rights information to consumers with ongoing relationships.

SB 354 also adds more granularity to the consent framework. Certain core insurance uses may proceed without consumer choice, and certain joint marketing, cross-marketing, and affiliate sharing are subject to an *opt-out* regime similar to the traditional GLBA/IIPPA approach, but use of personal information for other marketing activities,

.....

research activities and otherwise unenumerated purposes generally requires *affirmative opt-in consent* of the individual under SB 354. Likewise, sensitive personal information receives separate restrictions and considerations. And in all cases, consent must be *specific and recordable*; for example, the statute requires separate choices for purposes subject to opt-in or opt-out rights.

SB 354 also establishes an outright prohibition on commercialization of data: *covered entities may not sell consumer personal information for monetary or other valuable consideration*. This is a significant departure from the opt-out model embodied in CCPA and the revised model law under consideration at the National Association of Insurance Commissioners (“NAIC”) (see below) and will require that covered entities carefully review all of their data-sharing arrangements.

Two other areas will have important practical implications:

- First, data retention becomes an affirmative governance obligation, under which covered entities must maintain written retention policies and schedules and retain information only as reasonably necessary and proportionate. Beginning January 1, 2032, covered entities must review those policies and their data holdings at least every three years and securely destroy, delete, or deidentify information that is no longer needed, subject to legal-retention, fraud and claims-history exceptions.
- Second, SB 354 substantially raises expectations for third-party risk management. For example, covered entities must exercise due diligence in selecting and overseeing service providers and maintain written oversight procedures. And contracts must specify processing purposes, data categories and duration and require confidentiality, security safeguards, incident reporting, deletion, assistance with consumer requests, subcontractor flow-down obligations, purpose limitations and termination rights where a provider cannot comply. These statutory contract requirements will apply to contracts executed, amended or renewed after July 1, 2028.

Enforcement can include penalties of at least \$5,000 per knowing or should-have-known violation, subject to an aggregate \$1 million cap, with higher penalties for violation of cease-and-desist orders and certain limited judicial remedies for consumers.

SB 354 Compliance: Where to Start

Because many details remain subject to California Insurance Commissioner regulations, the near-term exercise is less about rewriting policies than about identifying where SB 354 creates decisions or dependencies, particularly those that may require significant time to resolve. Among the questions covered entities should consider are:

- Scope and segmentation. What entities are covered now that were not covered before? What data is covered now that was not covered before? Do any exceptions, exemptions, or other carve-outs apply?
- Data collection, purposes, and consent. Does the entity have a robust data inventory detailing what data is collected, why, and whether consent has been obtained where necessary? Which existing uses will be

subject to additional consent requirements under SB 354? Can existing consent systems record purpose-specific elections and withdrawals?

- Vendor management. Which vendors process covered information, which subcontractors do they use, and which agreements will be executed, amended or renewed after July 1, 2028? Who will bear responsibility for consumer requests, deletion, security incidents and evidence of compliance?
- Data retention. Do the entity's legacy policies and platforms contemplate the kind of information deletion requirements established in SB 354? Will the policies or platforms need to be changed?

Critically, many of these obligations will be brand new for third-party service providers that historically have not been directly regulated or subject to privacy laws like IIPPA.

SB 354 and NAIC: Where Is This Going?

SB 354 arrives at essentially the same moment that the NAIC is considering revisions to Model Law 672—Privacy of Consumer Financial and Health Information. Adopted in the wake of GLBA's enactment, Model Law 672 does not reflect many of the modern privacy protections or concepts that have been adopted into laws like CCPA over the last decade. The NAIC Privacy Protections (H) Working Group released a revised Model Law 672 draft on July 24, 2026, and the public comment period closed on September 22, 2026. The draft addresses many of the same issues as SB 354—e.g., reworking the notice-and-consent framework, more explicit coverage of third-party service-provider agreements, restrictions on sale and disclosure, and special treatment of sensitive personal information—though the details differ in several key respects.

NAIC's work on this issue demonstrates that SB 354 is not an isolated California experiment. Instead, it is part of a broader recognition among insurance regulators of the limitations of the traditional GLBA-era framework. The final NAIC framework is likely to differ from SB 354 in meaningful respects, and any model law will ultimately require state adoption before it becomes law. Nevertheless, insurers that operate nationally will not be well-served by a compliance strategy scattered across fifty (or more) jurisdictions. As with CCPA, SB 354 has become an important reference point for national compliance architecture that will likely spill over into other states as NAIC completes its work on revising Model Law 672.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez

202 303 1125

dalvarez@willkie.com

Stephanie Duchene

310 855 3066

sduchene@willkie.com

Laura E. Jehl

202 303 1056

ljehl@willkie.com

WILLKIE

BRUSSELS CHICAGO DALLAS FRANKFURT HAMBURG HOUSTON LONDON LOS ANGELES
MILAN MUNICH NEW YORK PALO ALTO PARIS ROME SAN FRANCISCO WASHINGTON

Copyright © 2026 Willkie Farr & Gallagher LLP. All rights reserved.

This alert is provided for educational and informational purposes only and is not intended and should not be construed as legal advice, and it does not establish an attorney-client relationship in any form. This alert may be considered advertising under applicable state laws. Our website is: www.willkie.com.