

California Enacts Sweeping New Insurance Privacy Law: What Insurers Need to Know About CIIPPA (SB 354)

WRITTEN BY

Theodore P. Augustinos | Kim Phan | Roshni Patel | Alexander R. Cox

KEY POINTS

- California's Senate Bill 354 enacted the California Insurance Information and Privacy Protection Act (CIIPPA), replacing the original Insurance Information and Privacy Protection Act and becoming operative July 1, 2028.
- The CIIPPA applies to insurance department licensees, surplus line insurers, reinsurers, and their third-party service providers, while excluding HIPAA-covered entities, title insurance, and certain Gramm-Leach-Bliley Act-regulated institutions without separate insurance licensure, among other entity and product exclusions.
- The CIIPPA requires insurers to deliver a stand-alone initial privacy notice generally within 21 calendar days after first collecting, processing, or sharing a consumer's personal information, among other new notice obligations.
- The CIIPPA establishes a structured opt-in and opt-out sharing framework that flatly prohibits the sale of personal information, among other new consumer-sharing protections.
- Third-party service providers under the CIIPPA must report security incidents, including breaches as defined under California's data breach law, directly to the Insurance Commissioner, generally within 30 days of discovery, among other vendor and breach-reporting requirements.

EXECUTIVE SUMMARY

On September 27, 2026, the governor of California signed into law Senate Bill 354, which replaces California's decades-old Insurance Information and Privacy Protection Act (IIPPA). The new insurance-specific privacy regime will be known as the California Insurance Information and Privacy Protection Act (CIIPPA). Combining concepts of Model Acts 670 and 672 promulgated by the National Association of Insurance Commissioners, the IIPPA was enacted in 1980 and has been occasionally updated since. CIIPPA imports much of the architecture and many concepts of the California Consumer Privacy Act (CCPA), California's comprehensive privacy law, but tailors them specifically to insurance underwriting, servicing, claims, and related data practices. The CIIPPA will become operative July 1, 2028, giving insurers a limited period of time to build out compliance.

The CIIPPA will require insurers to redesign consumer-facing notices, classify data-sharing uses, administer new opt-in and opt-out choices, update retention and deletion practices, and revise vendor terms. It also establishes a direct breach-reporting channel to the Insurance Commissioner and materially increases the potential consequences of noncompliance, including civil penalties reaching into seven figures for repeat violations. The practical work will cut across privacy, claims, underwriting, producer management, information security, procurement, and legal functions, making this an enterprise-wide undertaking.

The headline requirements are

- a stand-alone initial privacy notice generally due within 21 days after a licensee first collects, processes, or shares a consumer's personal information;
- an annual notice provided to a consumer during an ongoing relationship;
- a new sharing framework that combines permitted transaction-related disclosures with opt-in and opt-out requirements for other uses;
- enhanced consumer rights, including new rights to delete personal information and to be free from retaliation for exercising privacy rights; and
- vendor provisions that require service providers to report security incidents directly to the Commissioner as well as to the licensee.

These changes call for a new, enterprise-level compliance program rather than an incremental update to a legacy privacy disclosure.

BACKGROUND AND SCOPE

A Modernized Statute for Insurance Data

By replacing the IIPPA, the CIIPPA modernizes a statutory framework that had not been substantively updated since 1980 and 2002. The California Legislature identified an insurance-sector gap in the broader California privacy regime: the CCPA exempted consumer insurance-related information (*i.e.*, personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA)) and therefore did not comprehensively regulate the industry's collection, use, sharing, and protection of consumer data. The IIPPA implemented standards for the collection, use, and disclosure of personal information gathered during insurance transactions, but without the CCPA's comprehensive protections. The CIIPPA responds with a tailored regime that carries forward many principles from the IIPPA while layering in CCPA requirements focused on data minimization, retention and destruction discipline, third-party oversight, reasonable notice, breach governance, and protection against retaliation for consumers who exercise privacy rights.

The CIIPPA mandates new privacy regulations to be promulgated by the Insurance Commissioner by January 1, 2029. Nonetheless, the statute provides a clear basis for beginning a gap assessment now.

Who and What the CIIPPA Covers

The CIIPPA applies to insurance department licensees, surplus line insurers, reinsurers, and their third-party service providers. It broadly covers personal lines interactions involving applicants, policyholders, claimants, and beneficiaries. Commercial lines are also implicated to the extent a claim is brought by an individual claimant pursuing a claim under a commercial policy for personal, family, or household purposes. For group plans, notices required by the CIIPPA may be delivered to the employer rather than to each participant.

The statute includes important entity and product exclusions, including for Health Insurance Portability and Accountability Act (HIPAA)-covered entities and business associates; title insurance; and SEC-regulated or depository institutions subject to the GLBA where there is no separate insurance licensure. These exclusions require careful entity-by-entity and data-flow analysis; they should not be assumed to exempt a multi-line

enterprise from CIIPPA requirements altogether simply because one line of business qualifies for an exclusion.

The CIIPPA defines personal information expansively as information “processed or shared in the business of insurance 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.” The definition reaches familiar identifiers and insurance records as well as biometric information, neural data, and sensitive personal information. Insurers should therefore inventory data sources beyond traditional policy-administration and claims systems, including digital intake tools, analytics environments, fraud systems, and vendor-hosted platforms.

NEW NOTICE OBLIGATIONS

Initial and Annual Privacy Notices

The CIIPPA requires a clear and conspicuous, **stand-alone** privacy notice **within 21 calendar days** after the first collection, processing, or sharing of a consumer’s personal information. The notice obligation is not limited to a completed sale; applicants and claimants are also considered “consumers.” Existing customers must also receive a compliant notice at renewal or reinstatement or upon a new processing or sharing event if they have not already received one.

The statute recognizes limited exceptions. For example, an insurer is not required to provide notice to an applicant if a policy is not issued and the applicant’s personal information is not further processed. In connection with group policies, notice need only be provided to an employer, rather than plan participants. Other exceptions to the notice obligation include certain beneficiaries, emergency contacts, and other third-party individuals whose information is used solely to complete the transaction.

The CIIPPA separately requires notice at least annually during an ongoing business relationship, reflecting current privacy policies and practices. The annual notice may be combined with the initial notice, and is not required for former consumers or most claimants and other exempt categories. This dual notice framework means insurers should design a durable notice delivery infrastructure capable of tracking triggers, timing, and documentation across the life of a policy, rather than treating the initial notice as a one-time onboarding document.

Claimants and Investigative Reports

Claimants are expressly included in the definition of consumer. A claim (by someone other than a policyholder) therefore generally triggers the initial notice obligation, and a change in privacy practices during a pending claim can require an updated notice. Claims intake, first notice of loss, and third-party administrator workflows will need to be evaluated for timely delivery and evidence of delivery.

The CIIPPA independently requires advance notice to consumers, including claimants, before an investigative consumer report is prepared in connection with a claim. Workers’ Commercial business is generally excluded for most purposes of the statute, but an individual claimant becomes a consumer when making a claim primarily for personal, family, or household purposes. Commercial line carriers should therefore not assume exemption from the statute.

SHARING, UNDERWRITING, AND CONSUMER RIGHTS

A Structured Opt-In and Opt-Out Framework

The CIIPPA replaces prior, more ad hoc sharing rules with a structured approach. Subject to exceptions for authorized disclosure or transfer involving merger, acquisition, or bankruptcy, and in contrast with the CCPA, the CIIPPA defines sharing broadly as

sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by a licensee, surplus line insurer, reinsurer, or third-party service provider to a third party.

No consumer election is required when sharing is reasonably necessary and proportionate to an insurance transaction, compliance with law, protection of a policy interest, merger and acquisition activity, or group policyholder eligibility determinations. These permissions should not be read as blanket authorization, and the connection between the sharing and its permitted purpose should be documented.

Opt-in consent is required for specified marketing that is not otherwise permitted, certain research activities, and other purposes not disclosed to the consumer. Opt-out rights apply to joint marketing, cross-marketing of the licensee's own or affiliated products, specified affiliate sharing, and FAIR Plan clearinghouse activities. Sensitive personal information generally may not be shared outside enumerated exceptions without an opt-out opportunity. The result is a broad right to limit sharing that is not transactional or legally required, with opt-in reserved for higher-risk or less-expected uses. The CIIPPA also flatly prohibits the sale of personal information.

Operationally, insurers will need a data-use taxonomy that distinguishes transaction-related activity from marketing, research, affiliate, and other disclosures, and systems that capture, honor, record, and permit revocation of consumer choices. The statute does not define "specific marketing activity" or "specific research activity", making regulatory guidance especially important.

Adverse Underwriting Decisions and Expanded Rights

The CIIPPA preserves rights to access and correct personal information and to receive notice of adverse underwriting decisions, while adding a right to delete personal information and a right against retaliation for exercising statutory privacy rights. It also requires data-minimization practices and a written records-retention policy and schedule. Insurers will need a documented governance process that reconciles deletion requests against litigation holds, insurance record requirements, fraud investigations, and state retention mandates.

Under the statute, a licensee must provide specific reasons for an adverse underwriting decision in writing, or advise the consumer that written reasons are available on request. For declinations, cancellations, and nonrenewals involving specified property, automobile, and individual life, health, and disability policies, the specific reasons must accompany the decision. Consumers have 90 business days to seek additional detail, and the licensee has 21 business days to respond. The statute further identifies information that may not be used as a basis for an adverse underwriting decision. Templates, reason-code governance, and service-level controls should be reviewed together.

VENDOR MANAGEMENT, BREACH REPORTING, AND ENFORCEMENT

Third-Party Service Provider Requirements

Vendor contracting is also a central CIIPPA compliance issue. Agreements with third-party service providers must address confidentiality, administrative and technical safeguards, deletion obligations, subcontractor flow-down, and cooperation with the licensee's compliance efforts. Existing contract inventories should be mapped to the personal information each provider receives, processes, stores, or can otherwise access. Given the CIIPPA's mandate of clear instructions in third-party contracts, licensees, surplus line insurers, and reinsurers will very likely need to update language in all their vendor contracts.

Most significantly, contracts must require a service provider to report a security incident promptly, including a breach as defined in California's data breach law, to both the licensee and the Insurance Commissioner. This direct Commissioner-reporting duty is a meaningful departure from the traditional incident-response model, in which notification to the regulator often flowed only through the insurer. It should be embedded in new contracts and in amendment or renewal plans for legacy arrangements well before the effective date.

Incident Response and Penalties

The CIIPPA defines breaches by reference to California's existing data breach statute. Licensees, surplus line insurers, reinsurers, and third-party service providers must report breaches promptly, generally within 30 days of discovery, to the Insurance Commissioner. Producers must report breaches to both the insurer and the Commissioner. Incident response playbooks should therefore identify the responsible reporting entity for each scenario, assign Commissioner-notification ownership, account for vendor escalation, and preserve the facts needed to assess the 30-day timeline.

The enforcement provisions raise the cost of delay. Civil penalties begin at \$5,000 per violation and may reach \$1 million in the aggregate for multiple violations. Violating a cease-and-desist order carries a minimum \$15,000 fine per violation, increasing to \$50,000 per violation if the Commissioner finds a general business practice of noncompliance. Knowingly and willfully obtaining information under false pretenses can also be charged as a misdemeanor, punishable by a fine of up to \$50,000, up to six months in county jail, or both.

RECOMMENDED NEXT STEPS

Insurers should use the period through 2027 to conduct a focused CIIPPA gap assessment. Priorities include mapping personal information flows and sharing arrangements against the new permission, opt-in, and opt-out categories; comparing current notices with the new content and timing requirements; identifying claimant-facing and workers' compensation touchpoints; and reviewing service-provider agreements, particularly incident-reporting provisions. Insurers operating in other highly regulated states, such as New York, may be able to leverage existing asset inventories and other information maintained in compliance with New York's Cybersecurity Regulation (or others) to support these requirements.

During the 2027 through mid-2028 build phase, organizations should:

- draft stand-alone initial and annual notices;
- design and test notice delivery protocols;
- implement recordable and revocable consent and opt-out mechanisms;
- update retention policies and schedules;

- amend or renegotiate applicable vendor agreements;
- update adverse-decision templates and workflows to meet the 90-business-day and 21-business-day timelines; and
- train relevant personnel, including underwriting, claims, privacy and security, and producer relationships, on the expanded definitions and new notice triggers.

Finally, organizations should establish an incident protocol that includes direct Commissioner notification, monitoring for regulations that may extend obligations to producers by January 1, 2029, and follow related developments under SB 354 concerning investigative consumer reports and adverse underwriting decisions.

* * * * *

CIIPPA compliance will require scoped assessment that identifies high-volume data uses and contracts requiring early action. Our [Privacy + Cyber](#) team is available to assist with notice drafting, vendor amendments, and compliance program design. Please contact [Ted Augustinos](#), [Kim Phan](#), [Roshni Patel](#), [Alex Cox](#), or Alanna O'Reilly with questions.

**Alanna O'Reilly, an associate with Troutman Pepper Locke who is not yet licensed to practice law in any jurisdiction (application pending for admission to the Connecticut Bar), also contributed to this article.*

RELATED INDUSTRIES + PRACTICES

- [Insurance + Reinsurance](#)
- [Privacy + Cyber](#)