COMPLIANCE MAP · PART 1 OF 9

// ART-DAT-008 · PUBLISHED 23 NOVEMBER 2026

SaaS Compliance Basics: Three Questions Choose the Rules

The United States has no single privacy law. Three questions choose the stack a web SaaS product answers to: what kind of data it holds, whose data it is, and what role the company plays.

Jason Newell · MAX Research Collective · Article ART-DAT-008 · Published 23 November 2026
Licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/
Original: https://www.maxresearchcollective.com/articles/saas-compliance-basics.html
Cite as: Newell, J. (2026). SaaS Compliance Basics: Three Questions Choose the Rules. MAX Research Collective, ART-DAT-008. https://www.maxresearchcollective.com/articles/saas-compliance-basics.html

Part 1 of 9 in the series The Compliance Map for Web SaaS.

General information, not legal advice. Legal information current as of 22 November 2026. Laws, rules and court orders change, so check each date and threshold against the cited source before relying on it, and have a qualified lawyer review anything built or published from this map.

How to read the marks. A bracketed number points to a primary source in the sources appendix that was opened for this edition. A dagger marks a statement that names its law but whose text wasn't opened on a primary source for this edition. A dagger with a number (†6) points to the secondary reference in the secondary appendix that the statement came from, which is a law-firm alert, a tracker or trade press and never a primary source. A dagger alone (†) marks a statement that is considered but not known: it's kept so the rule stays in view, it has no reference behind it, and it hasn't been confirmed. (2026) marks a rule that is new, or first due, in 2026.

Where this part starts

A web SaaS product answers to a stack of privacy, health and payment laws, and three questions choose which ones: what kind of data it holds, whose data it is, and what role the company plays. One record can fall under three regimes at once, and the strictest rule for each control wins.

1. The short version

The United States has no single privacy law. A web SaaS product answers to a stack of them, chosen by three questions: what kind of data it holds, whose data it is (which state, which country, a child, a patient, a cardholder), and what role the company plays (the one who decides how data is used, or a vendor acting for someone who does).

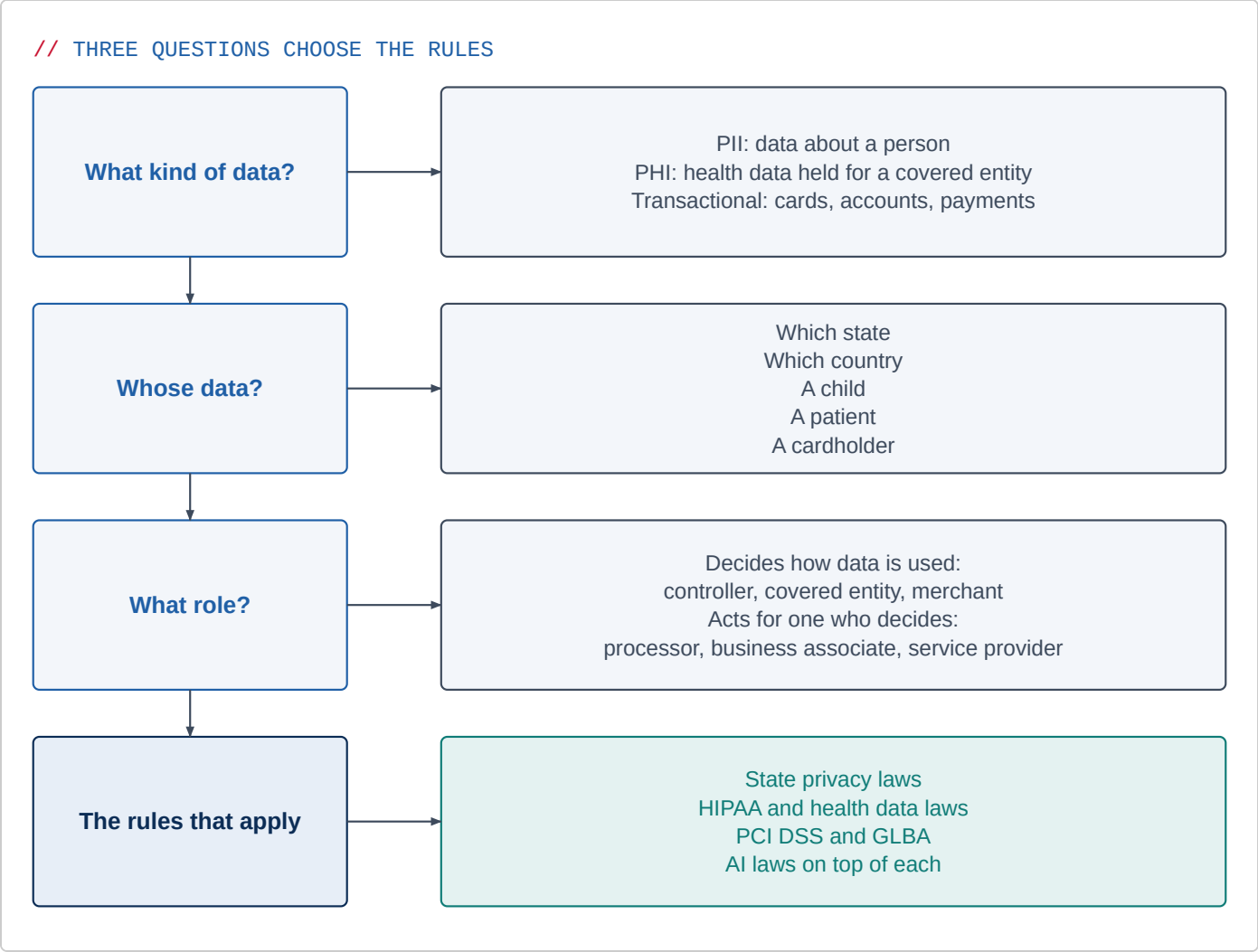


Figure 1. Three questions, answered top to bottom, select the rule set in the last box.

Table 1. The rule stack by kind of data.

IF YOU HOLD	THE CORE RULES ARE	THE REGULATOR OR ENFORCER
PII (any data about an identifiable person)	FTC Act § 5, state comprehensive privacy laws (20 in force, 4 more by 2028), breach laws in all 50 states, plus topic laws (children, biometrics, email, texts, video, wiretap)	FTC, state attorneys general, California's privacy agency, private plaintiffs under a few statutes
PHI (health data held for a covered entity)	HIPAA Privacy, Security and Breach Notification Rules; 42 CFR Part 2; state medical privacy laws; for health data outside HIPAA, the FTC's Health Breach Notification Rule and state consumer health data laws	HHS Office for Civil Rights, FTC, state attorneys general, private plaintiffs in Washington
Transactional data (payments, accounts, financial records)	PCI DSS (a contract, not a statute), GLBA and its Safeguards Rule, NYDFS Part 500, Regulation E, Nacha rules, the Bank Secrecy Act, tax and audit record rules	Card brands and acquirers, FTC, CFPB, SEC, banking regulators, state financial regulators
Any of them, with AI	All of the above still apply, plus state AI laws (California, Colorado, Texas, Utah, Illinois, New York and others), the EU AI Act for EU reach, and sector rules for AI in health and credit	The same enforcers, plus new duties owed by "developers" and "deployers"

Five things hold across almost every regime:

1. Know what you hold and why. Keep a data inventory and a stated purpose for each kind of data.
2. Protect it in proportion to the harm. Use encryption at rest and in transit, access by role, multi-factor authentication, logging and tested backups.

3. Keep it only as long as needed, and no shorter than the law requires. Retention has floors and ceilings.
4. Give people their rights on a clock. People get access, correction, deletion and opt-out, and an answer within a set number of days.
5. Tell people when it goes wrong, on a clock. Breach notice deadlines run from 24 hours to 60 days.

AI doesn't replace any of this. It adds new places data goes (prompts, training sets, embeddings, logs at a model vendor), new things done with it (inference, automated decisions) and new laws about both.

2. Three kinds of data, three sets of rules

Table 2. PII, PHI and transactional data compared.

	PII	PHI	TRANSACTIONAL DATA
What it is	Information that identifies, relates to or can reasonably be linked to a person or household: name, email, device ID, IP address, precise location, inferences	Individually identifiable health information created or received by a covered entity or its business associate, about health, care or payment for care	Payment card data, bank account and routing numbers, transaction history, invoices, account balances, credit data
The legal term varies	”Personal information” (California), ”personal data” (most states, GDPR), ”nonpublic personal information” (GLBA)	”Protected health information” (HIPAA); ”consumer health data” (Washington, Nevada) for health data outside HIPAA	”Cardholder data” and ”sensitive authentication data” (PCI DSS); ”nonpublic personal information” (GLBA); ”covered data” (CFPB)
What makes it regulated	Who the person is (state of residence, age), how many people, and whether data is sold or used for targeted ads	Who holds it. The same blood-pressure reading is PHI at a clinic and not PHI in a consumer fitness app	The payment rail (card, ACH), and whether the company is a ”financial institution”
”Sensitive” subset	Health, race, religion, sexual orientation, immigration status, biometrics, genetics, precise location, children’s data, often financial account numbers. Usually needs opt-in consent	Substance use disorder records (Part 2), psychotherapy notes, reproductive health, HIV status, genetic data get extra state and federal protection	Full card number, CVV, PIN, track data; account credentials; Social Security numbers
De-identification exit	”De-identified” under state law: cannot reasonably be linked,	HIPAA Safe Harbor (remove 18 identifiers)	Truncation, tokenization and hashing take data

	PII	PHI	TRANSACTIONAL DATA
	with a public commitment not to re-identify and contracts that bind recipients	or Expert Determination	out of PCI scope when done to the standard

One record is often all three at once. A patient's copay charge is PHI (payment for care), PII (the patient) and cardholder data (the card). The strictest rule for each control wins.

3. Which laws apply to you: the role tests

Most duties attach to a role. Decide the role for each product and each data flow before reading any rule.

Table 3. The role each regime puts its duties on.

REGIME	THE ROLE WITH PRIMARY DUTIES	THE VENDOR ROLE	HOW A SAAS COMPANY USUALLY LANDS
HIPAA	Covered entity: health plan, clearinghouse, or provider that bills electronically	Business associate: creates, receives, maintains or transmits PHI for a covered entity. Subcontractors are business associates too	Business associate, bound by a business associate agreement (BAA) and directly liable under the Security Rule [13][14]
State privacy laws	Controller (in California, business): decides why and how data is processed, and meets a size threshold	Processor (California: service provider or contractor): acts on instructions under a contract	Processor for customer data, controller for its own users, marketing leads and website visitors [45]
GDPR and UK GDPR	Controller	Processor, with a written Article 28 agreement	The same split [55]
GLBA	Financial institution: significantly engaged in financial activities (lending, payments, tax preparation, account servicing, many fintechs)	Service provider to a financial institution	Either; a fintech SaaS is often a financial institution in its own right [31]
PCI DSS	Merchant: accepts cards	Service provider: stores, processes or transmits cardholder data for others, or can affect its security	Merchant for its own billing; service provider if customers' card data passes through it †
COPPA	Operator of a site or service directed to children under 13, or with actual knowledge it collects from them	Not a separate role; vendors are covered through the operator	Operator when the product is for children or schools [2]

REGIME	THE ROLE WITH PRIMARY DUTIES	THE VENDOR ROLE	HOW A SAAS COMPANY USUALLY LANDS
State and EU AI laws	Developer (EU: provider): builds or substantially modifies the AI system	Deployer: uses it to make or help make decisions	Often both: deployer of a model vendor's model, developer of the product built on it [53][56]

Common thresholds in state privacy laws. Most apply to a company that does business in the state and handles the personal data of 100,000 residents in a year, or 25,000 while earning a share of revenue from selling data. Several are lower (Delaware, New Hampshire, Maryland and Rhode Island at 35,000; Montana at 25,000). Texas and Nebraska apply to any company that isn't a small business. California applies at $25 million in annual revenue (indexed), or 100,000 consumers or households, or half of revenue from selling or sharing data. The four laws enacted in 2026 set their own thresholds, which this paragraph leaves out. [45]

Common exemptions. PHI under HIPAA is exempt at the data level in nearly every state privacy law. GLBA is exempt at the entity level in most states and at the data level in California, Oregon, Minnesota and a few others. Employee and business-to-business data are exempt everywhere except California. Nonprofits are exempt in most states, not in Colorado, Oregon, Delaware, New Jersey, Maryland or Minnesota (each with its own limits).

Why it matters

A company that answers the three questions late answers them during a sale or an incident, with a customer or a regulator waiting. The role decides who signs which contract and who notifies whom, so it's the first thing a buyer's lawyer checks. Every later part of this series starts from the answers given here.

Appendix B: the series

Section numbers run through the whole series, so a reference to a section outside this part points to the part that holds it.

- Part 1, SaaS Compliance Basics: sections 1, 2, 3.
- Part 2, Privacy Law for SaaS: sections 4, 5.
- Part 3, HIPAA for SaaS: sections 6.
- Part 4, Payment and Financial Data in SaaS: sections 7.
- Part 5, Security Controls for Regulated SaaS: sections 8, 9, 10.
- Part 6, Data Retention and Consent in SaaS: sections 11, 12, 13.
- Part 7, Breach Notification and Vendor Contracts for SaaS: sections 14, 15, 16, 17.
- Part 8, AI in Regulated SaaS: sections 18, 19, 20.
- Part 9, One Compliance Program for SaaS: sections 21, 22, 23.

Glossary

TERM	DEFINITION
ADMT	Automated decision-making technology: software that makes, or largely makes, a decision about a person. State rules attach notices and opt-outs to it.
Addressable	A HIPAA Security Rule safeguard that must be put in place, or replaced with a documented equivalent, when it is reasonable and appropriate.
BAA	Business associate agreement: the contract HIPAA requires between a covered entity and a vendor that handles PHI for it.
Business associate	A vendor that creates, receives, maintains or transmits PHI for a covered entity. Most health SaaS companies are one.
CDE	Cardholder data environment: the systems that store, process or transmit card data, and so fall inside PCI DSS scope.
Controller	Under GDPR and most state privacy laws, the company that decides why and how personal data is processed.
Covered entity	Under HIPAA, a health plan, a clearinghouse, or a provider that bills electronically.
De-identification	Removing or changing data so it can no longer reasonably be linked to a person, to the standard the governing law sets.
Deployer	Under AI laws, the company that uses an AI system to make or help make decisions.
Developer	Under AI laws, the company that builds or substantially modifies an AI system. The EU AI Act calls it the provider.
DPIA	Data protection impact assessment: the written risk review GDPR and many state laws require before risky processing.
ePHI	Electronic protected health information, the subject of the HIPAA Security Rule.

Newell, J. (2026). MAX Research Collective, ART-DAT-008. CC BY 4.0

TERM	DEFINITION
MFA	Multi-factor authentication: sign-in that needs two or more kinds of proof.
NPI	Nonpublic personal information: the customer data GLBA protects at a financial institution.
PCI DSS	Payment Card Industry Data Security Standard: the card brands' contract standard for anyone handling card data.
PHI	Protected health information: identifiable health information held by a covered entity or its business associate.
PII	Personally identifiable information: data that identifies or can reasonably be linked to a person. Statutes call it personal information or personal data.
Processor	A vendor that handles personal data only on a controller's instructions. California calls it a service provider or contractor.
RAG	Retrieval-augmented generation: a model answering from documents fetched at the time of the question, usually through an embedding index.
SAQ	Self-assessment questionnaire: the form a smaller merchant or service provider uses to validate PCI DSS compliance.
Sensitive authentication data	The card security code, full track data and PIN. PCI DSS bars storing it after authorization.
SOC 2	An independent auditor's report on a service company's security and related controls.
Subprocessor	A vendor's own vendor that also handles the customer's data.
Tokenization	Replacing a card or account number with a stand-in value that is useless outside the system that issued it.

Appendix D: primary sources cited in this part

Each entry was opened on the issuing body's own site between 20 and 22 November 2026. The numbers are the same in every part of the series.

- [2] COPPA: 15 U.S.C. §§ 6501-6502; COPPA Rule, 16 CFR 312.2, 312.5, 312.8, 312.10; final rule amendments, FR Doc. 2025-05904 (effective 2025-06-23, compliance by 2026-04-22)
  - federalregister.gov
- [13] HIPAA Security Rule, 45 CFR 164.306, 164.308, 164.310, 164.312, 164.314, 164.316
  - ecfr.gov · part 164
- [14] HIPAA Privacy Rule, 45 CFR 164.502(b), 164.504(e), 164.508, 164.514, 164.520, 164.522, 164.524, 164.526, 164.528, 164.530(j)
  - ecfr.gov · part 164
- [31] FTC Safeguards Rule, 16 CFR 314.2, 314.4, 314.5
  - ecfr.gov · part 314
- [45] State privacy thresholds: 6 Del. C. ch. 12D; N.H. RSA 507-H:2; Md. Code, Com. Law § 14-4702; R.I. Gen. Laws § 6-48.1-4; Mont. Code § 30-14-2803; Tex. Bus. & Com. Code ch. 541; Neb. Rev. Stat. § 87-1103
  - delcode.delaware.gov · title6
- [53] Colorado SB 26-189, Automated Decision-Making Technology
  - leg.colorado.gov · bills
- [55] GDPR, Regulation (EU) 2016/679, arts. 3, 5, 7, 9, 12, 17, 20-22, 27, 28, 30, 32-35, 44, 46, 83
  - eur-lex.europa.eu · reg
- [56] EU AI Act, Regulation (EU) 2024/1689, arts. 99 and 113, as amended by Regulation (EU) 2026/1744 (OJ L, 2026-07-24)
  - eur-lex.europa.eu · reg

DATA ART-DAT-008

// ABOUT THE AUTHOR

Jason Newell leads organizations and people in technology, and is a researcher, deep technologist and builder — from a CRAY to agentic AI. He founded MAX Research Collective to build AI for regulated industries that runs where its owner has control, with healthcare as its strongest focus. About Jason → Connect on LinkedIn → ORCID →