COMPLIANCE MAP · PART 3 OF 9

// ART-DAT-010 · PUBLISHED 25 NOVEMBER 2026

HIPAA for SaaS: Addressable Is Not Optional

A SaaS company that handles patient data for a provider or a health plan is a business associate, and it carries the HIPAA Security Rule directly. Health data outside HIPAA is covered by the FTC and by state consumer health laws, which carry consent rules and, in Washington, a private right to sue.

Jason Newell · MAX Research Collective · Article ART-DAT-010 · Published 25 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/hipaa-for-saas.html
Cite as: Newell, J. (2026). HIPAA for SaaS: Addressable Is Not Optional. MAX Research Collective, ART-DAT-010. https://www.maxresearchcollective.com/articles/hipaa-for-saas.html

Part 3 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

6. PHI: HIPAA and everything around it

6.1 The HIPAA rules

Table 1. The four HIPAA rules.

RULE	CORE REQUIREMENTS	FOR A SAAS BUSINESS ASSOCIATE
Privacy Rule (45 CFR 164 Subpart E)	PHI is used and disclosed only for treatment, payment, health care operations, as the law requires, or with the patient's authorization; minimum necessary for everything but treatment; patient rights of access, amendment and accounting	Use PHI only as the BAA permits. No use for the vendor's own product improvement, analytics or model training unless the BAA says so and the law allows it [14]
Security Rule (Subpart C)	Administrative, physical and technical safeguards for electronic PHI: risk analysis, workforce training, access control, audit controls, integrity, transmission security, contingency plan	Directly liable. The risk analysis is the item OCR cites most in enforcement [13]
Breach Notification Rule (Subpart D)	Notice to individuals without unreasonable delay, at most 60 days; to HHS at the same time when 500 or more people are affected, and to the media when more than 500 residents of one state are	Notify the covered entity, at most 60 days by rule, usually far less by contract [15]
Enforcement Rule	Four penalty tiers, per violation, with annual caps adjusted for inflation; state attorneys general may also sue	No private right of action, but state negligence claims use HIPAA as the standard of care [16]

6.2 What changed, and what is still pending

Table 2. HIPAA changes and pending items on 2026-11-22.

ITEM	STATUS ON 2026-11-22
Privacy Rule final rule (2026)	Published 2026-11-19 (91 FR 74848). Shortens the right-of-access deadline from 30 days to 15 calendar days, with one extension of up to 30 calendar days, adjusts the fees allowed for copies, changes the Notice of Privacy Practices and defines personal health applications, among changes meant to support coordinated care. Effective 2027-01-19, compliance by 2027-07-19. Until then the 30-day rule stands [17]
Security Rule overhaul	Still a proposal. The January 2025 proposal would make encryption and multi-factor authentication required rather than "addressable", and add an asset inventory, network map, 72-hour restoration, annual compliance audits and vulnerability scans every six months. HHS's agenda now targets July 2027 for a final rule. The current Security Rule remains in force [18]
42 CFR Part 2 (substance use disorder records)	Aligned with HIPAA for consent, breach notice and penalties; compliance was due 2026-02-16 (2026). One consent can now cover treatment, payment and operations, but Part 2 records still cannot be used against the patient in legal proceedings without consent or a court order [19]
Reproductive health care privacy rule (2024)	Vacated nationwide by a federal court in Texas in June 2025. State laws now carry this protection [69]
Online tracking guidance	OCR's position that an IP address on a public health web page is PHI was vacated in part in 2024. Tracking on logged-in pages and patient portals remains a HIPAA problem, and state wiretap and health data laws cover the rest [20]
HTI-5 (2026)	Published 2026-10-28. Removes from EHR certification the "model card" source-attribute requirements for predictive decision support, effective 2026-12-28; the rule also proposed removing the risk-management requirement, which this edition didn't confirm in the final text. See § 19.3 [21]

6.3 Safeguards the Security Rule asks for

Table 3. Security Rule safeguards, required and addressable.

AREA	REQUIRED	ADDRESSABLE (ASSESS EACH ONE; IMPLEMENT IT IF REASONABLE AND APPROPRIATE, OR DOCUMENT WHY NOT AND ADOPT AN EQUIVALENT WHERE ONE IS REASONABLE)
Administrative	Risk analysis and risk management; sanction policy; activity review; a named security official; incident procedures; data backup, disaster recovery and emergency-mode plans; periodic evaluation; BAAs	Workforce clearance and termination procedures; security reminders; malware protection; log-in monitoring; password management; testing of contingency plans [13]
Physical	Workstation use and security; device and media disposal and re-use	Facility access controls; media accountability; backup before moving equipment [13]
Technical	Unique user identification; emergency access; audit controls; person or entity authentication	Automatic logoff; encryption at rest; integrity controls; encryption in transit [13]

”Addressable” isn’t ”optional”. For each addressable safeguard the company has to assess whether it is reasonable and appropriate in its own environment. If it is, the company implements it. If it isn’t, the company documents why, and implements an equivalent alternative where one is reasonable and appropriate [13]. Encryption is expected in practice. Lost or stolen PHI escapes breach notification only when it was encrypted as HHS guidance specifies (NIST SP 800-111 for data at rest; NIST SP 800-52, 800-77 or 800-113, or FIPS 140-2 validated processes, for data in transit) and the decryption key or process was not compromised. Anything else is unsecured PHI, and the notice rules apply [15]. The pending rule would make encryption mandatory.

6.4 Health data outside HIPAA

A wellness app, a symptom checker sold to consumers, a wearable, or a period tracker holds health data that HIPAA doesn't reach.

Table 4. Health data laws outside HIPAA.

LAW	REACH	REQUIREMENTS
FTC Health Breach Notification Rule (amended 2024)	Vendors of personal health records and related apps not covered by HIPAA	Notify individuals and the FTC within 60 days of a breach, which includes an unauthorized disclosure such as sharing with an ad platform without consent [22]
FTC Act § 5	The same companies	Orders against GoodRx, BetterHelp, Premom and others banned sharing health data for advertising [1][68]
Washington My Health My Data Act	Any company handling consumer health data of Washington residents or data processed in Washington; no size threshold	Separate consent to collect and to share; a signed authorization to sell; a ban on geofencing around health facilities; a standalone health privacy policy; a private right of action [23]
Nevada SB 370	Similar scope	Similar duties, enforced by the attorney general [24]
Connecticut, Virginia, Maryland	Through their privacy laws	Opt-in consent for consumer health data; limits on reproductive and sexual health data [25]
New York	The Health Information Privacy Act was vetoed in December 2025; a revised bill was introduced in 2026	Watch list [67]; revised bill †17
State medical privacy laws	California CMIA; Texas Medical Records Privacy Act (HB 300)	Often broader than HIPAA: Texas covers anyone who assembles or stores PHI and requires training; California covers apps that maintain medical information [26][64]
Texas SB 1188	Electronic health records of Texas patients	Records must be physically stored in the United States (from 2026-01-01),

LAW	REACH	REQUIREMENTS
		and practitioners must disclose AI use in diagnosis [26]; date †

6.5 Other health rules a SaaS product meets

Table 5. Other health rules that reach software.

RULE	WHY IT MATTERS
Information blocking (21st Century Cures Act)	Health IT developers, exchanges and providers may not interfere with access, exchange or use of electronic health information. Penalties up to $1 million per violation for developers. A vendor that slows or prices data export unreasonably is exposed [27]
Section 1557 (45 CFR 92.210)	Covered health programs must make reasonable efforts to identify and mitigate discrimination risk from patient care decision support tools, AI included; in force since 2025-05-01 [28]
FDA	Software that diagnoses or drives treatment may be a medical device. Clinical decision support is outside device regulation only when a clinician can independently review the basis for the recommendation [29]
CMS prior authorization and Medicare Advantage rules	An algorithm may assist, but coverage denials must rest on the individual's circumstances and be reviewed by a clinician [30]
Telehealth and prescribing	State licensure, DEA rules for controlled substances, and state consent rules apply to the service, and so to its software †

Why it matters

The first clinic to sign brings HIPAA with it, and the business associate agreement puts the breach clock on the vendor. The access deadline drops to 15 calendar days

on 2027-07-19, which is a product change as much as a policy one. A health feature in a wellness app can fall under Washington's law with no clinic involved at all.

Appendix A: 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-010. 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 C: 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.

- [1] 15 U.S.C. § 45 (FTC Act § 5)
  - govinfo.gov · uscode
- [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
- [15] HIPAA Breach Notification Rule, 45 CFR 164.402, 164.404, 164.406, 164.408, 164.410
  - ecfr.gov · part 164
- [16] HIPAA enforcement and preemption, 45 CFR 160.203, 160.404; 42 U.S.C. § 1320d-5(d)
  - ecfr.gov · part 160
- [17] HIPAA Privacy Rule final rule, 91 FR 74848, FR Doc. 2026-23429 (published 2026-11-19; effective 2027-01-19; compliance by 2027-07-19)
  - federalregister.gov
- [18] HIPAA Security Rule proposed rule, FR Doc. 2024-30983 (2025-01-06); final action date per the OIRA Unified Agenda, RIN 0945-AA22
  - federalregister.gov
- [19] 42 CFR Part 2, §§ 2.12, 2.16, 2.31; final rule, FR Doc. 2024-02544 (compliance by 2026-02-16)
  - federalregister.gov
- [20] HHS OCR, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, with notice of the 2024-06-20 court order
  - hhs.gov · hipaa online tracking

- [21] HTI-5 final rule, FR Doc. 2026-21943 (published 2026-10-28; effective 2026-12-28); 45 CFR 170.315(b)(11)
  - federalregister.gov
- [22] FTC Health Breach Notification Rule, 16 CFR 318.2, 318.4, 318.5; final rule, FR Doc. 2024-10855
  - ecfr.gov · part 318
- [23] Washington My Health My Data Act, RCW ch. 19.373
  - app.leg.wa.gov · RCW
- [24] Nevada consumer health data law, NRS 603A.400 to 603A.550
  - leg.state.nv.us · NRS 603A
- [25] Conn. Gen. Stat. ch. 743jj (§ 42-526); Va. Code § 59.1-200; Md. Code, Com. Law § 14-4707
  - cga.ct.gov · chap 743jj
- [26] Texas Health & Safety Code chs. 181 and 183
  - statutes.capitol.texas.gov
- [27] Information blocking, 42 U.S.C. § 300jj-52; 45 CFR 171.103; 42 CFR 1003.1410
  - govinfo.gov · uscode
- [28] Section 1557, 42 U.S.C. § 18116; 45 CFR 92.1(b), 92.210
  - ecfr.gov · part 92
- [29] FD&C Act § 520(o)(1)(E), 21 U.S.C. § 360j(o)(1)(E)
  - govinfo.gov · uscode
- [30] Medicare Advantage, 42 CFR 422.101(c), 422.566(d)
  - ecfr.gov · part 422
- [64] California: Civ. Code §§ 56.06, 1798.82, 1798.99.86, 1798.100, 1798.140, 1798.150; Penal Code § 637.2; Bus. & Prof. Code § 17602
  - leginfo.legislature.ca.gov · codes.xhtml
- [67] New York: Gen. Bus. Law §§ 349-a, 899-aa, 899-bb; S6953B of 2025 (RAISE Act, signed); S929 of 2025 (vetoed)
  - nysenate.gov · GBS

- [68] FTC press releases on GoodRx (2023-02), BetterHelp (2023-03), Premom (2023-05) and Everalbum (2021-05)
  - ftc.gov · ftc enforcement action bar goodrx sharing consumers sensitive health…
- [69] HHS OCR, HIPAA and Reproductive Health, with notice of the 2025-06-18 order in Purl v. HHS (N.D. Tex.)
  - hhs.gov · reproductive health

Appendix D: secondary references, not primary sources

A dagger with a number points here. Apart from the few agency pages among them, none is a primary source.

- †17 Consumer health data: Epstein Becker Green; Morrison Foerster; IAPP on Washington
  - ebglaw.com · new yorks health information privacy act poised to become the latest…
  - mofo.com · 260316 nyhipa returns in 2026 revised bill
  - iapp.org · washington my health my data act overview

DATA ART-DAT-010

// 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 →