

LINTEL VANTAGE

Vantage Baseline for Ashlar Health, Inc. • Q2 2026

Full node state as of 2026-05-17.

Specimen issue. Ashlar Health, Inc. is a fictional company; this issue is published as a sample of what Lintel Vantage produces.

THE LANDSCAPE

20 comprehensive state privacy laws in effect as of 2026-05-17 (counting laws enforceable statewide; 19 excluding narrower-scope statutes such as Florida's). Computed from the registry.

Nearest deadlines

Every date below already appears in this document's own statute tables, gathered here as a single sorted reference.

DATE	STATUTE	JURISDICTION	TYPE
2026-07-01	Connecticut Public Act 25-113 (privacy/CTDPA amendments)	US-CT	Effective
2026-07-01	Iowa utilization-review AI amendment (HF 2635 § 2, amending Iowa Code § 514F.8)	US-IA	Effective
2026-07-01	Iowa conversational-AI service requirements (SF 2417)	US-IA	Effective
2026-08-01	Connecticut Public Act 25-113 (privacy/CTDPA amendments)	US-CT	Compliance date
2027-01-01	CPPA regulations package (cyber audits, risk assessments, ADMT, insurance)	US-CA	Compliance date
2027-01-01	Colorado AI Act as replaced (SB 26-189)	US-CO	Compliance date
2027-01-01	Oklahoma comprehensive privacy statute (2026 enactment)	US-OK	Effective
2027-05-01	Alabama Personal Data Protection Act	US-AL	Effective
2027-07-01	Iowa conversational-AI service requirements (SF 2417)	US-IA	Compliance date

US Privacy Obligations

State and federal law governing the collection, use, disclosure, and protection of personal data.

State Comprehensive Privacy Laws

priv.comp

Cross-sector state statutes governing how covered entities process the personal data of that state's residents. Each statute applies on its own thresholds. Any count of these laws is stated with the convention behind it — what it counts, what it leaves out, and the date it was true — never as a bare number.

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-CA	California Consumer Privacy Act (as amended by CPRA) [oag.ca.gov]	In effect	2020-01-01	2023-01-01
US-VA	Virginia Consumer Data Protection Act [law.lis.virginia.gov] (source not independently confirmed)	In effect	2023-01-01	—
US-CO	Colorado Privacy Act [coag.gov]	In effect	2023-07-01	2024-07-01
US-CT	Connecticut Data Privacy Act [portal.ct.gov]	In effect	2023-07-01	2025-01-01
US-CT	Connecticut Public Act 25-113 (privacy/CTDPA amendments) [cga.ct.gov]	Enacted, effective in future	2026-07-01	2026-08-01
US-UT	Utah Consumer Privacy Act [le.utah.gov]	In effect	2023-12-31	—
US-TX	Texas Data Privacy and Security Act [dir.texas.gov]	In effect	2024-07-01	—
US-OR	Oregon Consumer Privacy Act [doj.state.or.us]	In effect	2024-07-01	2026-01-01
US-FL	Florida Digital Bill of Rights [flsenate.gov]	In effect	2024-07-01	—
US-MT	Montana Consumer Data Privacy Act [dwt.com] (source not independently confirmed)	In effect	2024-10-01	—
US-DE	Delaware Personal Data Privacy Act [legis.delaware.gov]	In effect	2025-01-01	—
US-IA	Iowa Consumer Data Protection Act [legis.iowa.gov]	In effect	2025-01-01	—
US-NH	New Hampshire Data Privacy Act [gc.nh.gov]	In effect	2025-01-01	—

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-NJ	New Jersey Data Privacy Act [pub.njleg.state.nj.us]	In effect	2025-01-15	—
US-NE	Nebraska Data Privacy Act [nebraskalegislature.gov]	In effect	2025-01-01	—
US-TN	Tennessee Information Protection Act [tn.gov]	In effect	2025-07-01	—
US-MN	Minnesota Consumer Data Privacy Act [revisor.mn.gov]	In effect	2025-07-31	—
US-MD	Maryland Online Data Privacy Act [mgaleg.maryland.gov]	In effect	2025-10-01	2026-04-01
US-IN	Indiana Consumer Data Protection Act [iga.in.gov]	In effect	2026-01-01	—
US-KY	Kentucky Consumer Data Protection Act [apps.legislature.ky.gov]	In effect	2026-01-01	—
US-RI	Rhode Island Data Transparency and Privacy Protection Act [webserver.rilegislature.gov]	In effect	2026-01-01	—
US-AL	Alabama Personal Data Protection Act [alison.legislature.state.al.us] (source not independently confirmed)	Enacted, effective in future	2027-05-01	—
US-OK	Oklahoma comprehensive privacy statute (2026 enactment) [oklegislature.gov] (source not independently confirmed)	Enacted, effective in future	2027-01-01	—

WHY THIS MATTERS

Comprehensive state privacy statutes govern how a covered entity collects, uses, discloses, and protects the personal data of that state's residents. Each statute applies on its own jurisdictional and numeric thresholds, and the statutes differ in vocabulary and scope. This area is relevance-routed on the presence of residents in any state; the statutes listed are the full monitored set of comprehensive state privacy laws enacted as of this document's date, not a set narrowed to the states a Company Profile names. Inclusion is neither a determination that a statute's thresholds are met nor an indication that its state matches the profile: a listed statute may govern a state where an entity has no residents, and a state named in a profile may have no comprehensive statute at all, or one whose enactment post-dates this document.

VOCABULARY The CCPA speaks of a "business" and a "service provider"; the Virginia-model statutes speak of a "controller" and a "processor." Both vocabularies are carried; they are never conflated.

Breach-Notification Duties

priv.breach

A breach-notification duty exists in every US state and under several federal rules: notice to affected individuals, and in some cases to regulators, after a security breach meeting the statute's definition. The federal rules are tracked here in full; state duties are tracked through amendments in monitored states rather than as a standing digest of all fifty. The duty is triggered by an incident, not by a company attribute; it is therefore carried for every subscriber.

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-FED	GLBA Safeguards Rule (16 CFR Part 314), breach-report amendment [ftc.gov]	In effect	2024-05-13	—
US-FED	FTC Health Breach Notification Rule (16 CFR Part 318), revised [federalregister.gov]	In effect	2024-07-29	—

COVERAGE

Amendments to state breach statutes are surfaced through the legislative backbone for monitored states; a 50-state breach-law digest is NOT claimed. Bounded on the What We Monitor page.

Consumer Health Data Laws

priv.sect.health

State statutes protecting health-adjacent data held by entities outside HIPAA, with broad definitions of consumer health data; Washington's statute carries a private right of action.

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-WA	Washington My Health My Data Act (Ch. 19.373 RCW) [atg.wa.gov]	In effect	2024-03-31	2024-06-30
US-NV	Nevada consumer health data law (SB 370) [leg.state.nv.us]	In effect	2024-03-31	—

FTC Act Section 5

priv.fed.ftc5

Federal authority over unfair or deceptive acts or practices in commerce, applied to privacy misrepresentations and data-security failures. It reaches virtually all commercial actors.

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-FED	FTC Act Section 5 (15 U.S.C. §45) [uscode.house.gov]	In effect	—	—

Health Breach Notification Rule

priv.fed.hbnr

The federal rule requiring breach notice by vendors of personal health records and related entities not covered by HIPAA, as revised in 2024.

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-FED	FTC Health Breach Notification Rule (16 CFR Part 318), revised [federalregister.gov]	In effect	2024-07-29	—

Profiling / Automated Decision-Making

admt.profiling

Processing that evaluates individuals by automated means, or that makes or substantially replaces human decision-making in decisions with legal or similarly significant effects. Regulated as a privacy matter under the state comprehensive statutes and the CPPA's ADMT regulations, and as AI governance under the Colorado-model consequential-decision regimes.

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-CA	CPPA regulations package (cyber audits, risk assessments, ADMT, insurance) [coppa.ca.gov]	In effect	2026-01-01	2027-01-01
US-CO	Colorado AI Act as replaced (SB 26-189) [leg.colorado.gov]	In effect	2026-05-14	2027-01-01

WHY THIS MATTERS

Where automated decision-making tools are used to make or substantially replace significant decisions about individuals, several state regimes — notably the CPPA regulations and Colorado's SB 26-189 — attach notice, opt-out, and assessment duties.

VOCABULARY CPPA: "ADMT" and "significant decision." Virginia model: "profiling" with "legal or similarly significant effects." Colorado: "covered ADMT." Each term is used only with its home framework named.

Cross-referenced under: [priv.comp](#) · [ai.consequential](#)

ADMT Risk / Impact Assessment

admt.riskassessment

Assessment duties triggered by automated decision-making or significant-decision processing; the CPPA regulations require a risk assessment, the Colorado regime an impact assessment.

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-CA	CCPA regulations package (cyber audits, risk assessments, ADMT, insurance) [cppa.ca.gov]	In effect	2026-01-01	2027-01-01
US-CO	Colorado AI Act as replaced (SB 26-189) [leg.colorado.gov]	In effect	2026-05-14	2027-01-01

WHY THIS MATTERS

Where covered automated decision-making technology is used to make or substantially replace significant decisions, several regimes attach a documented assessment duty in addition to notice and opt-out duties — a risk assessment under the CCPA regulations and an impact assessment under Colorado SB 26-189.

Cross-referenced under: [priv.comp.dpa](#) · [ai.consequential](#)

Definitions and mechanics

Applicability Thresholds · Each statute sets its own scope through resident-count, revenue, and share-of-revenue-from-sale tests; the numeric triggers differ by state.

Data-Level Exemptions · Data already governed by the GLBA, HIPAA, or FCRA, and data processed in employment or business-to-business contexts, is carved out of most state statutes. California is the outlier: the CCPA reaches employee and B2B data.

Shifting Definitions · Core statutory terms — personal data, sale, share, sensitive data, profiling, targeted advertising, consumer — carry materially different meanings across states; "sale" is money-only in some states and money-or-other-value in others, and "consumer" excludes employees under the Virginia model but not under the CCPA.

Consumer Rights · Statutes grant residents enumerated rights — access, correction, deletion, portability, opt-outs from sale, targeted advertising, and profiling — with an appeal mechanism where a request is refused.

Consent Mechanics · Statutes condition certain processing on consent — typically opt-in for sensitive data and minors' data — and prohibit obtaining consent through dark patterns.

WHY THIS MATTERS

Where an entity processes categories the state statutes treat as sensitive data, most comprehensive regimes require opt-in consent and prohibit obtaining that consent through dark patterns.

Universal Opt-Out Signals · Many statutes require covered entities to honor a universal opt-out preference signal, such as the Global Privacy Control, transmitted by a consumer's browser or device.

Controller / Processor Duties · Statutes impose duties on the processing relationship itself: contracts with processors (service providers, under the CCPA), purpose limitation, data minimization, and reasonable security.

Data Protection / Risk Assessments · Statutes require a documented assessment before or for certain processing activities — targeted advertising, sale, profiling, sensitive data, and other heightened-risk processing. The Virginia model calls this a data protection assessment; the CPPA regulations call it a risk assessment.

Privacy Notice Content · Statutes prescribe the categories of disclosure a privacy notice must contain.

Enforcement Mechanics (cure / penalties / rulemaking) · Each statute sets its own enforcement machinery: cure periods (several of which expired in 2025–26), attorney-general rulemaking authority, per-violation penalties, and — rarely — a private right of action.

US AI-Governance Obligations

State and federal law governing the development and deployment of artificial-intelligence systems.

Consequential / High-Risk Decision Systems

ai.consequential

Statutes governing AI systems that make, or materially influence, consequential decisions — employment, credit, housing, insurance, healthcare, education — under Colorado SB 26-189 and comparable regimes. Colorado's regime speaks of developers and deployers; Illinois regulates employers.

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-CO	Colorado AI Act as replaced (SB 26-189) [leg.colorado.gov]	In effect	2026-05-14	2027-01-01
US-CO	Colorado AI Act, original (SB 24-205) [leg.colorado.gov]	Repealed before effect	—	—
US-IL	Illinois employment-AI amendments (HB 3773 / PA 103-0804) [ilga.gov]	In effect	2026-01-01	—

WHY THIS MATTERS

Where AI systems make or materially influence consequential decisions — employment, credit, housing, insurance, healthcare, or education — the Colorado-model developer-and-deployer regimes (SB 26-189) allocate documentation, notice, and review duties.

VOCABULARY Anchor every term to its home framework — "covered ADMT" under Colorado SB 26-189 is not "ADMT" under the CPPA regulations.

Developer vs Deployer Duties

ai.devdeploy

Statutes allocate duties by actor role — those who build a system and those who put it to use — but the role vocabulary is not stable across states (developer/deployer under Colorado SB 26-189, frontier developer, employer, user).

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-CO	Colorado AI Act as replaced (SB 26-189) [leg.colorado.gov]	In effect	2026-05-14	2027-01-01
US-TX	Texas Responsible AI Governance Act (HB 149) [capitol.texas.gov]	In effect	2026-01-01	—

AI Interaction Disclosure

ai.transparency

Duties to disclose that a consumer is interacting with an AI system rather than a human, triggered in some states only for defined higher-risk interactions.

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-UT	Utah AI Policy Act (SB 149, as amended by SB 226) [le.utah.gov]	In effect	2025-05-07	—
US-CA	California companion chatbot law (SB 243) [gov.ca.gov]	In effect	2026-01-01	2027-07-01
US-TX	Texas Responsible AI Governance Act (HB 149) [capitol.texas.gov]	In effect	2026-01-01	—
US-ID	Idaho Conversational AI Safety Act (SB 1297) [legislature.idaho.gov]	Enacted, effective in future	2027-07-01	—
US-IA	Iowa conversational-AI service requirements (SF 2417) [legis.iowa.gov]	Enacted, effective in future	2026-07-01	2027-07-01

WHY THIS MATTERS

Where a consumer-facing chatbot or AI assistant is offered to the public, several states — including Utah under SB 149, California under SB 243, and Texas under HB 149 — require disclosure that the interaction is with an AI system rather than a human, with the triggering conditions and required disclosure cadence differing by statute.

VOCABULARY The statutes here disclose the same kind of fact under different actor vocabularies, and the words are not interchangeable. Three of them regulate an "operator," and it is a different actor in each: under California SB 243 an operator is a person who makes a companion chatbot platform available to a user in the state (Business and Professions Code section 22601); under Idaho SB 1297 it is the operator of a conversational AI service under Idaho Code title 48, chapter 21; under Iowa SF 2417 it is the operator defined by Iowa Code chapter 554J. The word is never used here without naming which act it belongs to. Texas HB 149 speaks of a developer and a deployer — its own vocabulary, not the Colorado SB 26-189 developer/deployer pairing that shares the words. Utah SB 149's disclosure duties fall on a "supplier," a term Utah's Chapter 75 takes from the Utah Consumer Sales Practices Act rather than coining. No term above travels without its home framework in the same sentence.

Prohibited AI Uses

ai.prohibited

Categorical statutory bans on developing or deploying AI for named intentional harmful purposes; intent-based, with disparate impact alone insufficient under the Texas statute.

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-TX	Texas Responsible AI Governance Act (HB 149) [capitol.texas.gov]	In effect	2026-01-01	—

Sectoral AI — Health / Mental Health

ai.sectoral.health

AI-specific rules in healthcare and mental-health contexts, split between use-restriction and disclosure models.

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-TX	Texas health-context AI provisions (SB 1188) [capitol.texas.gov]	In effect	2025-09-01	2026-01-01
US-IL	Illinois mental-health AI restrictions (HB 1806) [ilga.gov]	In effect	2025-08-01	—
US-IA	Iowa utilization-review AI amendment (HF 2635 § 2, amending Iowa Code § 514F.8) [legis.iowa.gov]	Enacted, effective in future	2026-07-01	—

WHY THIS MATTERS

Where artificial intelligence is used in a health-care context, sectoral statutes impose duties that differ by model: Texas's SB 1188 follows a disclosure approach, while Iowa's amendment to Iowa Code § 514F.8 restricts an AI-based algorithm or system from being the sole basis to deny, delay, or downgrade a medical-necessity prior-authorization request.

Profiling / Automated Decision-Making

admt.profiling

Processing that evaluates individuals by automated means, or that makes or substantially replaces human decision-making in decisions with legal or similarly significant effects. Regulated as a privacy matter under the state comprehensive statutes and the CPPA's ADMT regulations, and as AI governance under the Colorado-model consequential-decision regimes.

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-CA	CPPA regulations package (cyber audits, risk assessments, ADMT, insurance) [coppa.ca.gov]	In effect	2026-01-01	2027-01-01
US-CO	Colorado AI Act as replaced (SB 26-189) [leg.colorado.gov]	In effect	2026-05-14	2027-01-01

WHY THIS MATTERS

Where automated decision-making tools are used to make or substantially replace significant decisions about individuals, several state regimes — notably the CPPA regulations and Colorado's SB 26-189 — attach notice, opt-out, and assessment duties.

VOCABULARY CPPA: "ADMT" and "significant decision." Virginia model: "profiling" with "legal or similarly significant effects." Colorado: "covered ADMT." Each term is used only with its home framework named.

Cross-referenced under: [priv.comp](#) · [ai.consequential](#)

ADMT Risk / Impact Assessment

admt.riskassessment

Assessment duties triggered by automated decision-making or significant-decision processing; the CPPA regulations require a risk assessment, the Colorado regime an impact assessment.

■ WATCHED SUBJECT TO INSTABILITY

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-CA	CPPA regulations package (cyber audits, risk assessments, ADMT, insurance) [coppa.ca.gov]	In effect	2026-01-01	2027-01-01
US-CO	Colorado AI Act as replaced (SB 26-189) [leg.colorado.gov]	In effect	2026-05-14	2027-01-01

WHY THIS MATTERS

Where covered automated decision-making technology is used to make or substantially replace significant decisions, several regimes attach a documented assessment duty in addition to notice and opt-out duties — a risk assessment under the CPPA regulations and an impact assessment under Colorado SB 26-189.

Cross-referenced under: [priv.comp.dpa](#) · [ai.consequential](#)

Enforcement Postures

Regulator investigation and enforcement activity under the statutes above.

Federal AI Preemption Watch

[fed-instability.eo14365](#)

Executive, agency, and litigation activity that may destabilize — not create — state AI obligations: Executive Order 14365, the DOJ AI Litigation Task Force and its suits, and the FCC and FTC preemption proceedings. None of it imposes a duty of its own. It is carried here because it may unsettle the state AI duties reported elsewhere in this document, and a duty whose footing is in question is worth knowing about before it moves.

JURISDICTION	STATUTE	STATUS	EFFECTIVE	COMPLIANCE DATE
US-FED	Executive Order 14365, "Ensuring a National Policy Framework for Artificial Intelligence" (90 Fed. Reg. 58499) [federalregister.gov]	In effect	2025-12-11	—

WHY THIS MATTERS

Executive Order 14365, the Department of Justice's AI Litigation Task Force, and related federal litigation may destabilize — without themselves creating — state AI-governance obligations, including through challenges to specific state statutes. This item does not itself impose or remove a duty; it flags that an affected framework's status may change and is worth continued attention.

Definitions and mechanics

State AG Privacy Enforcement · Attorney-general investigations, cure notices, lawsuits, and settlements under state privacy and AI statutes. Coverage is bounded to a named subset of the most active offices.

COVERAGE

Named subset: CA, TX, CT, CO, OR, NJ (see sources.yaml)

WHY THIS MATTERS

State attorneys general bring investigations, cure notices, lawsuits, and settlements addressing privacy and AI-related practices under consumer-protection and state privacy statutes. Coverage in this product is bounded to a named subset of the most active offices; an enforcement item reflects activity in a monitored jurisdiction, not a finding about any particular company's practices.

CPPA / California AG Enforcement · California Privacy Protection Agency and California Department of Justice sweeps, orders, and settlements, including Delete Act / DROP activity.

WHY THIS MATTERS

The California Privacy Protection Agency and the California Department of Justice bring administrative orders, sweeps, and settlements under the California Consumer Privacy Act and its implementing regulations, including matters concerning the Delete Act and DROP. An enforcement item reflects a specific agency action, not a determination about any other company's compliance.

FTC Enforcement · Federal Trade Commission actions under Section 5, COPPA, the GLBA Safeguards Rule, and the Health Breach Notification Rule.

RELEVANCE

Items appear in this Baseline because your Company Profile indicates a matching condition. This is relevance-routing, not a determination of applicability.

COVERAGE

This Baseline draws on our monitored sources. It does not claim to reflect all changes affecting your organization.

SOURCING

Citations link to the specific document supporting a claim wherever a stable public copy of it exists; otherwise they link to the official government page for that instrument.

Lintel Vantage is a regulatory-change monitoring product for US software companies, published by Lintel Standard.