Chamber

CHAMBER CARDIO, INC.

COMPREHENSIVE PRIVACY POLICY

Effective Date: 03/01/2026| Last Updated: 03/01/2026 | Version: 1.0

Applies to: heartfirst.care and all associated services

Regulatory Coverage: HIPAA/HITECH • CCPA/CPRA (CA) • CDPA (VA) • CPA (CO) • CTDPA (CT) • UCPA (UT) • MCDPA (MT) • TDPSA (TX) • OCPA (OR) • NHPA (NH) • NCDPA (NC, pending) • MODPA (MD) • MPDPA (MN) • ICDPA (IA) • NDPA (NE) • JDPA (NJ) • DPDPA (DE) • INCDPA (IN) • KCP (KY) • TIPA (TN)

---

1. WHO WE ARE AND HOW THIS POLICY APPLIES

Chamber Cardio, Inc. ("Chamber," "we," "us," or "our") provides care coordination, health navigation, and wellness support services to patients with cardiovascular conditions. Chamber is not a clinical provider and does not practice medicine. This Privacy Policy governs how Chamber collects, uses, discloses, and protects personal information and Protected Health Information ("PHI") in connection with our services, including our website at heartfirst.care.

Our Role in Your Care

Chamber operates primarily as a care coordination intermediary. This means we work alongside your health care providers and health plans — not in place of them. Most patients who interact with Chamber do so because their health plan, health care provider, or other Covered Entity has referred or enrolled them in a Chamber program. In those cases, Chamber receives your health information from that Covered Entity in accordance with its own Notice of Privacy Practices and applicable law, including HIPAA. Chamber uses that information solely to provide the services for which you have been referred or enrolled.

You may also interact with Chamber directly through heartfirst.care, including by completing our heart health assessment tool. Information you provide through that tool or through direct contact with our care coordination team is also governed by this Policy.

Our Role Under HIPAA

When Chamber creates, receives, maintains, or transmits PHI on behalf of a Covered Entity, we act as a Business Associate under HIPAA (45 CFR Part 164). In this role, we are bound by a fully executed Business Associate Agreement ("BAA") with each Covered Entity partner. PHI processed under a HIPAA BAA is exempt from state consumer privacy laws listed in this Policy.

Chamber

When Chamber collects personal information directly from you — for example, through heartfirst.care or the heart health assessment — we may act as a Covered Entity in our own right with respect to that information. In either case, your PHI is protected under HIPAA and our HIPAA Notice of Privacy Practices, available here.

---

2. STATE PRIVACY LAW MASTER REFERENCE TABLE

The table below summarizes all currently enacted US state comprehensive privacy laws covered in this Policy.

State	Law / Acronym	Effective Date	Opt-Out of Sale?	Sensitive Data Consent?	Private Right of Action?	Enforcement
California	CCPA/CPRA	Jan 1, 2020 / Jan 1, 2023	Yes	Yes (CPRA)	Yes (data breaches)	CA AG + CPPA
Virginia	CDPA	Jan 1, 2023	Yes	Yes	No	VA AG
Colorado	CPA	Jul 1, 2023	Yes	Yes	No	CO AG
Connecticut	CTDPA	Jul 1, 2023	Yes	Yes	No	CT AG
Utah	UCPA	Dec 31, 2023	Yes	No (notice only)	No	UT AG
Texas	TDPSA	Jul 1, 2024	Yes	Yes	No	TX AG
Oregon	OCPA	Jul 1, 2024	Yes	Yes	No	OR AG
Montana	MCDPA	Oct 1, 2024	Yes	Yes	No	MT AG
New Hampshire	NHPA	Jan 1, 2025	Yes	Yes	No	NH AG
New Jersey	JDPA	Jan 15, 2025	Yes	Yes	No	NJ AG
Delaware	DPDPA	Jan 1, 2025	Yes	Yes	No	DE AG
Iowa	ICDPA	Jan 1, 2025	Yes	No (notice only)	No	IA AG
Nebraska	NDPA	Jan 1, 2025	Yes	Yes	No	NE AG

Chamber

State	Law / Acronym	Effective Date	Opt-Out of Sale?	Sensitive Data Consent?	Private Right of Action?	Enforcement
Indiana	INCDPA	Jan 1, 2026	Yes	Yes	No	IN AG
Tennessee	TIPA	Jul 1, 2025	Yes	Yes	No	TN AG
Minnesota	MPDPA	Jul 31, 2025	Yes	Yes	No	MN AG
Maryland	MODPA	Oct 1, 2025	Yes	Yes	No	MD AG
Kentucky	KCP	Jan 1, 2026	Yes	Yes	No	KY AG
North Carolina	NCDPA	Pending (2026)	Yes	Yes	No	NC AG

Note on Applicability: Many state laws listed above apply only when a business meets specified consumer volume or revenue thresholds. Chamber's current applicability under each law depends on the number of state residents whose data Chamber processes and Chamber's revenue profile. Chamber's universal no-sale commitment (Section 5.2) satisfies opt-out requirements under all listed state laws regardless of threshold applicability. As Chamber expands nationally, additional state laws may become applicable. This Policy is designed to support that expansion.

---

3. INFORMATION WE COLLECT

3.1 How We Receive Your Information

Chamber receives personal information and PHI through the following channels:

From your health plan or health care provider. Your health plan, health care provider, or other Covered Entity may refer you to Chamber's program and share your health information with us in connection with that referral. This is the most common way Chamber receives patient information. Chamber uses this information solely to provide the services for which you have been referred or enrolled.

Directly from you. You may provide information when you visit heartfirst.care, complete the heart health assessment, or communicate with Chamber's care coordination team by phone, text, email, video conferencing, or other electronic means.

Through the heart health assessment. If you complete the heart health assessment or other wellness tools available through heartfirst.care, the information you provide and any outputs generated may constitute PHI and will be handled in accordance with this

Chamber

Policy and our HIPAA Notice of Privacy Practices. Results from these tools are for general health awareness purposes only and do not constitute a clinical evaluation or diagnosis.

Automatically through technology. When you visit heartfirst.care, we may automatically collect certain technical information about your device and browsing activity as described in Section 3.2 below.

3.2 Categories of Personal Information We Collect

Category	Examples	Source	Laws Requiring Disclosure
Identifiers	Name, email, phone number, date of birth, device ID (adults 18+ only)	You; Covered Entity referral	All state laws
Contact Data	Address, phone number	You; Covered Entity referral	All state laws
Health / PHI	Cardiovascular diagnoses, medications, lab results, treatment history, insurance information, heart health assessment responses and outputs	You; Covered Entity referral; assessment tool	HIPAA + all state laws (sensitive)
Usage / Interaction Data	Pages visited, features used, session duration, clickstream	Automatically collected	All state laws
Device / Technical Data	OS, browser type, screen resolution, referring URL, cookie identifiers	Automatically collected	All state laws
Communications	Care coordination notes, support correspondence, call and text records	You; care coordination interactions	All state laws
Inferences	Health awareness indicators derived from assessment responses (non-PHI, aggregated only)	Assessment tool	CA, CO, CT, VA, OR, MT, MN, MD

What We Do Not Collect: Chamber does not collect payment card information, full Social Security numbers, biometric data, or financial account credentials from patients

in connection with the heartfirst.care platform. Chamber does not bill patients directly for services.

---

4. HOW WE USE YOUR INFORMATION

Purpose	Legal Basis (HIPAA)	Legal Basis (State Laws)
Care coordination and health navigation support	HIPAA TPO	Contract performance
PHI processing on behalf of Covered Entities	45 CFR §164.504(e) BAA	HIPAA exemption applies
Heart health assessment delivery and follow-up	HIPAA TPO	Contract performance
Program enrollment and eligibility management	Legitimate operations	Contract; legitimate interest
Electronic and SMS communications	HIPAA TPO; TCPA consent	Contract; consent
AI-assisted care coordination and outreach prioritization	HIPAA TPO	Legitimate interest; consent where required
Security monitoring and incident response	Security Rule compliance	Legal obligation; legitimate interest
Product analytics (non-PHI, aggregated only)	De-identified data	Consent where required; legitimate interest
Legal and regulatory compliance	Legal obligation	Legal obligation
Customer and patient support	Operations	Contract; legitimate interest

We Will Never:

- Sell or share personal information or PHI with third parties for monetary or other valuable consideration
- Use PHI for targeted advertising or cross-context behavioral advertising
- Use sensitive personal information for purposes beyond providing the requested service

- Profile individuals based on health information for non-healthcare purposes
- Make automated decisions producing legal or significant clinical effects using PHI without appropriate human oversight

---

5. DISCLOSURE OF PERSONAL INFORMATION

5.1 Authorized Disclosures

We may disclose personal information and PHI in the following limited circumstances:

- To Covered Entities (health plans, health care providers) under applicable BAAs as directed and permitted by HIPAA, including to the Covered Entity that referred you to Chamber's program
- To subcontractors and vendors under BAAs and/or Data Processing Agreements (DPAs) who support our care coordination services
- To comply with applicable law, court orders, or valid legal process
- To HHS OCR for HIPAA compliance audits and investigations
- To state attorneys general or the California Privacy Protection Agency (CPPA) as required by law
- In connection with a merger, acquisition, or sale of assets, subject to equivalent privacy protections
- With your express written authorization for any other purpose

5.2 No Sale or Sharing of Personal Information

Universal No-Sale Commitment

Chamber does not sell, rent, trade, or otherwise transfer personal information or PHI to any third party for monetary or other valuable consideration. Chamber does not share personal information for cross-context behavioral advertising. This applies to all users regardless of state of residence and satisfies opt-out rights under CCPA/CPRA, CDPA, CPA, CTDPA, UCPA, TDPSA, OCPA, MCDPA, NHPA, JDPA, DPDPA, ICDPA, NDPA, INCDPA, TIPA, MPDPA, MODPA, KCP, and NCDPA.

No mobile information, including SMS opt-in data and consent, will be shared with third parties or affiliates for marketing or promotional purposes.

---

6. HIPAA / HITECH — FEDERAL HEALTH PRIVACY

Chamber

6.1 Business Associate and Covered Entity Roles

As described in Section 1, Chamber may act as a Business Associate when processing PHI on behalf of a Covered Entity partner, or may act as a Covered Entity in its own right when collecting PHI directly from patients through heartfirst.care and related services. In either capacity, Chamber is bound by HIPAA and its implementing regulations and maintains fully executed BAAs with all Covered Entity partners.

6.2 Technical and Administrative Safeguards for PHI

- AES-256 encryption for ePHI at rest; TLS 1.3 for data in transit
- Role-based access controls and multi-factor authentication (MFA)
- Annual HIPAA risk assessments and ongoing risk management
- Comprehensive workforce training and sanction policies
- Audit logging retained for minimum 6 years
- SOC 2 Type II certified infrastructure

6.3 Individual HIPAA Rights

Depending on whether Chamber is acting as a Business Associate or Covered Entity with respect to your PHI, some rights may need to be exercised through your health plan or health care provider rather than directly with Chamber. Please contact us at [privacy email] and we will direct your request appropriately.

Your HIPAA rights include:

- Access and copy of PHI (30 days; electronic format available under HITECH)
- Amendment of inaccurate or incomplete PHI
- Accounting of disclosures (6-year lookback)
- Restrictions on uses and disclosures
- Confidential communications by alternative means
- File complaints with HHS OCR: 1-800-368-1019 | www.hhs.gov/ocr

---

7. ARTIFICIAL INTELLIGENCE

As part of providing care coordination services, Chamber uses artificial intelligence ("AI") functionality to support outreach prioritization, identification of care gaps, risk stratification, and program effectiveness. AI functionality processes your health

information consistent with this Policy, our HIPAA Notice of Privacy Practices, and applicable law, including HIPAA.

Chamber employs AI functionality with appropriate testing, controls, and ongoing human oversight. AI-generated outputs inform — but do not independently determine — care coordination activities, and do not constitute clinical recommendations or diagnoses. Chamber does not use AI to make automated decisions that produce legal or significant clinical effects on patients without human review.

In connection with phone and SMS communications, Chamber complies with the FCC's February 2024 ruling that AI-generated voices constitute "artificial voices" under the TCPA, requiring prior express consent, identification disclosures, and opt-out mechanisms consistent with Section 9 of this Policy.

---

8. ELECTRONIC AND MOBILE COMMUNICATIONS

Chamber may communicate with you by phone, SMS text message, email, video conferencing, or other electronic means in connection with your care coordination program. These communications may include appointment reminders, care coordination updates, program information, and health navigation support.

SMS Communications. By providing your phone number to Chamber, or by having it provided on your behalf by a Covered Entity, you consent to receive SMS communications from Chamber at that number. SMS message frequency varies. You may opt out of SMS communications at any time by:

- Replying "STOP" to any text message
- Contacting us at [support email or phone] by any other reasonable means that clearly expresses your desire to stop receiving messages

Chamber will honor all opt-out requests within 10 business days of receipt. For assistance, text "HELP" or contact us at [support contact]. Message and data rates may apply.

Informational vs. Marketing Communications. Chamber's communications are informational in nature — they relate to your care coordination program and do not constitute marketing. Chamber does not use your PHI for marketing purposes and does not send promotional SMS messages. Consent to receive SMS communications is not a condition of receiving Chamber's services.

No Sharing of Mobile Data. SMS opt-in data and consent information will not be shared with any third parties or affiliates for marketing or promotional purposes.

Chamber

9. CALIFORNIA — CCPA / CPRA

Applies To

Law: California Consumer Privacy Act (CCPA), Cal. Civ. Code §1798.100 et seq., as amended by the California Privacy Rights Act (CPRA)

Threshold: Businesses that collect PI of 100,000+ CA consumers/households OR derive 50%+ of revenue from selling PI OR have $25M+ gross annual revenue

Enforcement: California AG + California Privacy Protection Agency (CPPA)

HIPAA Exemption: PHI processed under HIPAA BAA is exempt per Cal. Civ. Code §1798.145(c)

Your California Rights

Right to Know (Access): Request the categories and specific pieces of PI collected about you, sources, business purposes, and categories of third parties receiving your PI. Response within 45 days (extendable by 45 days with notice).

Right to Delete: Request deletion of PI we hold about you, subject to exceptions including legal obligations and HIPAA retention requirements.

Right to Correct (CPRA): Request correction of inaccurate PI. We will use commercially reasonable efforts to correct the data.

Right to Opt Out of Sale / Sharing: We do not sell or share PI. If this changes, a "Do Not Sell or Share My Personal Information" link will appear on our homepage.

Right to Limit Use of Sensitive PI (CPRA): Direct us to limit Sensitive PI use to what is necessary to provide the requested service.

Right to Non-Discrimination: We will not deny services, charge different prices, or provide different quality because you exercised a CCPA/CPRA right.

Sensitive PI Under CPRA: SSN / government ID numbers; account log-in credentials; precise geolocation; racial/ethnic origin; religious/philosophical beliefs; union membership; contents of communications; genetic data; biometric data; health / sex life / sexual orientation data.

How to Submit a California Privacy Request

Email: [PRIVACY EMAIL] Toll-Free Phone: [PHONE] Online Portal: heartfirst.care/privacy-request Authorized Agent Requests: Provide signed written

authorization; direct consumer verification may be required. Response Time: Acknowledged within 10 business days; fulfilled within 45 days (extendable by 45 days).

---

10. VIRGINIA — CONSUMER DATA PROTECTION ACT (CDPA)

Applies To

Law: Consumer Data Protection Act (CDPA) (Va. Code Ann. §59.1-575 et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 50%+ revenue from sale of PI

Enforcement: Virginia AG (no private right of action)

HIPAA Exemption: PHI under HIPAA BAA is exempt per Va. Code Ann. §59.1-578(B)

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and profiling • Appeal (60 days; escalate to VA AG)

Sensitive Data Categories: Racial/ethnic origin • Religious beliefs • Mental/physical health diagnoses • Sexual orientation/gender identity • Citizenship/immigration status • Genetic/biometric data • PI of known children • Precise geolocation

Key Provisions: Data Protection Assessments required for high-risk processing; opt-out honored within 15 days; appeal mechanism required.

---

11. COLORADO — COLORADO PRIVACY ACT (CPA)

Applies To

Law: Colorado Privacy Act (CPA) (C.R.S. §6-1-1301 et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 25%+ revenue from sale of PI

Enforcement: Colorado AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt per C.R.S. §6-1-1304(2)(a)

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and profiling • Appeal (60 days)

Key Provisions: Must honor Global Privacy Control (GPC) signals; Data Protection Assessments required; two or more opt-out methods required; consent required for secondary use of sensitive data.

12. CONNECTICUT — CONNECTICUT DATA PRIVACY ACT (CTDPA)

Applies To

Law: Connecticut Data Privacy Act (CTDPA) (Conn. Gen. Stat. §42-515 et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 25%+ revenue from sale of PI

Enforcement: Connecticut AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, profiling • Appeal (60 days)

Key Provisions: Must honor GPC opt-out signals; consent required for sensitive PI; Data Protection Assessments required; 60-day cure period before enforcement.

---

13. UTAH — UTAH CONSUMER PRIVACY ACT (UCPA)

Applies To

Law: Utah Consumer Privacy Act (UCPA) (Utah Code Ann. §13-61-101 et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 50%+ revenue from PI sale, AND $25M+ annual revenue

Enforcement: Utah AG via Utah Division of Consumer Protection

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Delete (of data you provided) • Data Portability • Opt Out of sale and targeted advertising

Key Provisions: No right to correct; sensitive data requires opt-out rather than opt-in; no data protection assessment requirement; no right to appeal; 30-day cure period.

---

14. TEXAS — TEXAS DATA PRIVACY AND SECURITY ACT (TDPSA)

Applies To

Law: Texas Data Privacy and Security Act (TDPSA) (Tex. Bus. & Com. Code §541 et seq.)

Consumer Threshold: Conducts business in TX or targets TX consumers; no size threshold

Enforcement: Texas AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and profiling • Appeal (60 days)

Key Provisions: No revenue or consumer volume threshold; must honor universal opt-out mechanisms including GPC; Data Protection Assessments required; 30-day cure period; small business exemption available.

---

15. OREGON — OREGON CONSUMER PRIVACY ACT (OCPA)

Applies To

Law: Oregon Consumer Privacy Act (OCPA) (ORS §646A.570 et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 25%+ revenue from sale of PI

Enforcement: Oregon AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and profiling • Right to know list of third parties receiving PI • Appeal (45 days)

Key Provisions: One of the broadest sensitive data category definitions; controllers must respond to third-party PI list requests; Data Protection Assessments required; privacy notice required at or before collection; 10-day breach notification (one of the shortest in the US).

---

16. MONTANA — MONTANA CONSUMER DATA PRIVACY ACT (MCDPA)

Applies To

Law: Montana Consumer Data Privacy Act (MCDPA) (Mont. Code Ann. §30-14-3001 et seq.)

Consumer Threshold: 50K consumers/year OR 25K consumers and derive 25%+ revenue from sale of PI

Enforcement: Montana AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and profiling • Appeal (60 days)

Key Provisions: Lower consumer threshold (50K) than most states; sensitive data requires opt-in consent; Data Protection Assessments required.

---

17. NEW HAMPSHIRE — NEW HAMPSHIRE PRIVACY ACT (NHPA)

Applies To

Law: New Hampshire Privacy Act (NHPA) (RSA §507-H)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 25%+ revenue from sale of PI

Enforcement: New Hampshire AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and profiling • Appeal (60 days)

Key Provisions: Must honor GPC universal opt-out signals; Data Protection Assessments required; 60-day cure period; 72-hour breach notification if 500+ NH residents affected.

---

18. NEW JERSEY — NEW JERSEY DATA PRIVACY ACT (JDPA)

Applies To

Law: New Jersey Data Privacy Act (JDPA) (N.J.S.A. §56:8-166.1 et seq.)

Consumer Threshold: 100K consumers/year (excluding payment processing data) OR 25K consumers and derive 25%+ revenue from PI sale

Enforcement: New Jersey AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and automated decision-making profiling • Appeal (60 days)

Key Provisions: Must honor GPC and similar universal opt-out signals; sensitive data requires opt-in consent; Data Protection Assessments required; 72-hour breach notification (one of the strictest).

---

19. DELAWARE — DELAWARE PERSONAL DATA PRIVACY ACT (DPDPA)

Applies To

Law: Delaware Personal Data Privacy Act (DPDPA) (6 Del. C. §12D-101 et seq.)

Consumer Threshold: 35K consumers/year OR 10K consumers and derive 20%+ revenue from PI sale

Enforcement: Delaware AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and automated profiling • Appeal (60 days)

Key Provisions: Lower thresholds (35K/10K) increase applicability; protects children under 18 (broader than COPPA's under-13 standard); sensitive data requires opt-in consent; Data Protection Assessments required.

---

20. IOWA — IOWA CONSUMER DATA PROTECTION ACT (ICDPA)

Applies To

Law: Iowa Consumer Data Protection Act (ICDPA) (Iowa Code §715D)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 50%+ revenue from sale of PI

Enforcement: Iowa AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (90 days) • Delete (of PI you provided) • Data Portability • Opt Out of sale of PI

Key Provisions: Narrower rights than most states — no right to correct, no right to opt out of targeted advertising; sensitive data requires opt-out rather than opt-in; 90-day cure period before enforcement.

---

21. NEBRASKA — NEBRASKA DATA PRIVACY ACT (NDPA)

Applies To

Law: Nebraska Data Privacy Act (NDPA) (LB1074 (2024))

Consumer Threshold: Applies to businesses that process PI of NE consumers and meet size criteria

Enforcement: Nebraska AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and automated profiling • Appeal (60 days)

Key Provisions: Sensitive data requires opt-in consent; Data Protection Assessments required; must honor universal opt-out mechanisms.

---

22. INDIANA — INDIANA CONSUMER DATA PROTECTION ACT (INCDPA)

Applies To

Law: Indiana Consumer Data Protection Act (INCDPA) (Ind. Code §24-15 et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 50%+ revenue from sale of PI

Enforcement: Indiana AG (30-day cure period)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and profiling • Appeal (60 days)

Key Provisions: Effective January 1, 2026; sensitive data requires opt-in consent; Data Protection Assessments required; substantially modeled after Virginia CDPA.

---

23. TENNESSEE — TENNESSEE INFORMATION PROTECTION ACT (TIPA)

Applies To

Law: Tennessee Information Protection Act (TIPA) (Tenn. Code Ann. §47-18-3201 et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 50%+ revenue from sale of PI, AND $25M+ annual revenue

Enforcement: Tennessee AG (15-day cure period)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and automated profiling • Appeal (60 days)

Key Provisions: Unique bona fide privacy program safe harbor — entities with documented privacy programs receive a compliance defense; sensitive data requires opt-in consent; 15-day cure period (shortest of all states).

---

24. MINNESOTA — MINNESOTA CONSUMER DATA PRIVACY ACT (MPDPA)

Applies To

Law: Minnesota Consumer Data Privacy Act (MPDPA) (Minn. Stat. §325O et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 25%+ revenue from sale of PI

Enforcement: Minnesota AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and automated profiling • Right to question automated decision-making • Appeal (60 days)

Key Provisions: Effective July 31, 2025; right to question and opt out of solely automated decisions broader than most states; human review required for certain automated decisions; sensitive data requires opt-in consent; Data Protection Assessments required.

---

25. MARYLAND — MARYLAND ONLINE DATA PRIVACY ACT (MODPA)

Applies To

Law: Maryland Online Data Privacy Act (MODPA) (Md. Code Com. Law §14-4601 et seq.)

Consumer Threshold: 35K consumers/year OR 10K consumers and derive 20%+ revenue from sale of PI

Enforcement: Maryland AG (no private right of action)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (60 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and automated profiling • Appeal (60 days)

Key Provisions: One of the strongest state laws — prohibits processing sensitive PI unless strictly necessary for the service; cannot sell sensitive data at all; effective October 1, 2025; protects children under 18 (broader than COPPA); lower threshold (35K/10K) increases applicability.

Note for Chamber: Maryland is part of Chamber's core DC/MD/VA service geography. Given MODPA's lower consumer threshold and broader children's privacy protections, Chamber should treat Maryland compliance as a current priority regardless of whether the 35K threshold has been met.

---

26. KENTUCKY — KENTUCKY CONSUMER DATA PROTECTION ACT (KCP)

Applies To

Law: Kentucky Consumer Data Protection Act (KCP) (KRS §367.400 et seq.)

Consumer Threshold: 100K consumers/year OR 25K consumers and derive 50%+ revenue from sale of PI

Enforcement: Kentucky AG (30-day cure period)

HIPAA Exemption: PHI under HIPAA is exempt

Consumer Rights: Access (45 days) • Correct • Delete • Data Portability • Opt Out of sale, targeted advertising, and automated profiling • Appeal (60 days)

Key Provisions: Effective January 1, 2026; substantially modeled after Virginia CDPA; sensitive data requires opt-in consent; Data Protection Assessments required.

---

27. NORTH CAROLINA — NC DATA PRIVACY ACT (NCDPA) [PENDING]

Applies To

Law: NC Data Privacy Act (NCDPA) [Pending] (HB 335 / SB 525 (as of 2025))

Consumer Threshold: Expected: 100K consumers/year OR 25K consumers with 25%+ revenue from sale of PI

Enforcement: North Carolina AG (expected)

HIPAA Exemption: PHI under HIPAA expected to be exempt

Expected Consumer Rights: Access • Correct • Delete • Portability • Opt-Out (sale, targeted advertising, profiling) • Appeal

Key Provisions: Pending as of early 2025; expected to be among the most consumer-friendly of Southern state laws; this section will be updated upon enactment. Chamber recommends building compliance infrastructure in advance of passage.

---

28. UNIVERSAL OPT-OUT MECHANISMS (GPC)

Several state laws — including Colorado (CPA), Connecticut (CTDPA), Texas (TDPSA), New Hampshire (NHPA), New Jersey (JDPA), and Nebraska (NDPA) — require businesses to honor universal opt-out mechanisms such as the Global Privacy Control (GPC) signal.

Chamber honors the GPC browser signal as an opt-out of sale and sharing of personal information for cross-context behavioral advertising. When we detect a GPC signal from your browser, we will automatically treat your visit as an opt-out request without requiring any additional action on your part. To enable GPC, use a compatible browser or browser extension that supports the GPC specification at globalprivacycontrol.org.

---

29. COOKIES AND TRACKING TECHNOLOGIES

Chamber uses limited tracking technologies on heartfirst.care. We do not use marketing or behavioral advertising cookies on any pages where health information is collected or displayed.

Cookie Type	Purpose	Required?	Retention
Strictly Necessary	Session management, security, form functionality. Cannot be disabled.	Yes	Session / up to 1 year
Functional / Preference	Language and display preferences. Disabling may impair features.	No	Up to 1 year
Analytics / Performance	Aggregated, anonymized usage data. No PHI collected via analytics tools.	No	Up to 13 months
Marketing / Advertising	Not used on heartfirst.care or any pages where health information is collected.	N/A	N/A

Upon first visit, a cookie consent banner allows you to accept all, accept only necessary, or customize by category. You may update preferences at any time via

[COOKIE PREFERENCES LINK]. GPC signals are honored as a cookie preference opt-out for applicable state residents.

Important: Chamber is committed to ensuring that no PHI entered through the heart health assessment or other health tools on heartfirst.care is accessible to analytics or tracking technologies. If you have questions about how your health information is protected from tracking tools, contact us at [privacy email].

---

30. CHILDREN'S PRIVACY

Chamber's services are intended solely for individuals who are 18 years of age or older. We do not knowingly collect, use, or disclose personal information from anyone under the age of 18, and the heartfirst.care site and all associated services are not directed to minors.

If you are under 18, please do not use the Services or submit any personal information through heartfirst.care.

COPPA Compliance: Chamber does not knowingly collect personal information from children under 13, consistent with the Children's Online Privacy Protection Act (COPPA), 16 CFR Part 312.

If we discover we have collected information from a minor: If Chamber becomes aware that it has inadvertently collected personal information from an individual under the age of 18, we will take prompt steps to delete that information from our records. If you believe we may have collected information from or about a minor, please contact us immediately at [privacy email].

Delaware and Maryland: Under the Delaware Personal Data Privacy Act (DPDPA) and Maryland Online Data Privacy Act (MODPA), enhanced protections apply to individuals under 18. Chamber's blanket exclusion of minors from the Services satisfies these requirements. Chamber does not sell the personal information of minors and does not direct advertising to minors.

---

31. DATA RETENTION

Data Type	Retention Period	Governing Law
PHI (Business Associate)	Per Covered Entity direction; minimum 6 years	HIPAA

Data Type	Retention Period	Governing Law
PHI (direct collection, including assessment data)	Minimum 6 years from date of collection or last service interaction	HIPAA
Care coordination records	Duration of program enrollment + 6 years	HIPAA
Communications records (calls, texts, emails)	3 years from last interaction	TCPA; state laws
Security and audit logs (ePHI)	Minimum 6 years	HIPAA Security Rule
Security logs (non-PHI)	3 years	Best practice
Website analytics (aggregated, non-PHI)	24 months, then deleted/anonymized	CCPA/CPRA; CPA; CTDPA
Consumer rights request records	5 years from request date	CCPA; CPA; CTDPA
Session cookies	End of browser session	All state laws
Persistent cookies	Up to 13 months from consent	CPRA; EU ePrivacy guidance

---

32. DATA SECURITY

Safeguard Category	Controls Implemented
Encryption	AES-256 at rest; TLS 1.3 in transit; FIPS 140-2 validated modules
Access Controls	Role-based access control (RBAC); least-privilege; MFA for all PHI access
Network Security	Zero-trust architecture; WAF; DDoS mitigation; network segmentation
Vulnerability Management	Annual penetration testing; continuous vulnerability scanning; patch management SLA
Monitoring	24/7 SIEM-based security monitoring; automated anomaly detection

Safeguard Category	Controls Implemented
Physical Security	SOC 2 Type II certified data centers; biometric access; 24/7 surveillance
Workforce Controls	Background screening; annual security training; NDAs; sanction policy
Vendor Management	Security assessments for all vendors; BAAs and DPAs required; periodic reviews
Incident Response	Documented IR plan; tabletop exercises annually; 24-hour initial response SLA

---

33. DATA BREACH NOTIFICATION

Jurisdiction	Law / Authority	Notification Deadline
Federal (PHI)	HIPAA/HITECH — HHS OCR	60 days to Covered Entity; CE notifies individuals and HHS
California	CCPA/CPRA — CA AG + CPPA	Expedient; AG if >500 residents affected
Virginia	CDPA / VA Breach Law — VA AG	Expedient notification
Colorado	HB 18-1128 — CO AG	30 days (AG); 30 days (consumers)
Connecticut	Conn. Gen. Stat. §36a-701b — CT AG	60 days
Utah	Utah Code §13-44-202 — UT AG	30 days
Texas	Tex. Bus. & Com. §521 — TX AG	Within 30 days; AG if >250 TX residents
Oregon	ORS §646A.604 — OR AG	Within 10 days (strictest in the US)
Montana	MCA §30-14-1704 — MT AG	30 days
New Hampshire	RSA §359-C:20 — NH AG	72 hours if >500 residents; 30 days otherwise

Jurisdiction	Law / Authority	Notification Deadline
New Jersey	JDPA / NJ Breach Law — NJ AG	72 hours (one of the strictest)
Delaware	DPDPA / 6 Del. C. §12B-102 — DE AG	60 days
Iowa	Iowa Code §715C.2 — IA AG	30 days
Nebraska	Neb. Rev. Stat. §87-803 — NE AG	30 days
Indiana	Ind. Code §24-4.9 — IN AG	45 days
Tennessee	Tenn. Code Ann. §47-18-2107 — TN AG	45 days
Minnesota	Minn. Stat. §325E.61 — MN AG	30 days (72 hours if >500 residents)
Maryland	MODPA / Md. Code §14-3504 — MD AG	45 days
Kentucky	KRS §365.732 — KY AG	30 days
North Carolina	N.C. Gen. Stat. §75-65 — NC AG	Without unreasonable delay (30 days guidance)

---

34. HOW TO EXERCISE YOUR PRIVACY RIGHTS

Submit a Privacy Rights Request

Email: [PRIVACY EMAIL] Toll-Free Phone: [PHONE NUMBER] Online Portal: heartfirst.care/privacy-request Mail: Chamber Cardio, Inc., 853 New Jersey Ave SE, STE 200, Washington, DC 20003, Attn: Privacy Officer

Response Times: We acknowledge all requests within 10 business days. Access / Portability / Correction / Deletion: Fulfilled within 45 days (extendable by 45 days with notice), except Iowa (90 days). Appeal: If we deny your request, you may appeal within 60 days. We will respond to appeals within 60 days. You may escalate denied appeals to your state Attorney General.

HIPAA Requests: For requests related to PHI that Chamber holds as a Business Associate on behalf of your health plan or health care provider, we may need to route

your request to the appropriate Covered Entity. We will advise you of the correct process within 10 business days of receiving your request.

---

35. CHANGES TO THIS PRIVACY POLICY

We update this Policy to reflect changes in applicable law, business practices, or technologies. Material changes are communicated via: (1) posting on heartfirst.care with a revised Last Updated date; (2) prominent notice on our homepage for 30 days; (3) email notification to patients with an active care coordination relationship; and (4) 30-day advance written notice to Covered Entity partners for PHI-related changes.

Continued use of the Services following notice of material changes constitutes your acceptance of the revised Policy. If you disagree with any changes, you should stop using the Services and contact us to discuss your options.

---

36. GOVERNING LAW

This Privacy Policy is governed by the laws of the State of Delaware, consistent with the Federal Arbitration Act and applicable federal privacy law, without regard to conflict of law provisions. Nothing in this section limits the rights of consumers under applicable state privacy laws.

---

37. CONTACT AND REGULATORY AUTHORITY INFORMATION

Privacy Officer

Company: Chamber Cardio, Inc.

Privacy Officer: [NAME / TITLE]

Address: 853 New Jersey Ave SE, STE 200, Washington, DC 20003

Email: [PRIVACY EMAIL]

Phone: [PHONE]

Portal: heartfirst.care/privacy-request

Key Regulatory Authorities

HHS OCR (HIPAA): 1-800-368-1019 | hhs.gov/ocr

California AG/CPPA: oag.ca.gov | cppa.ca.gov

Virginia AG: oag.state.va.us

Colorado AG: coag.gov

Connecticut AG: portal.ct.gov/ag

Maryland AG: marylandattorneygeneral.gov

Chamber

Privacy Officer

DPO (if applicable): [DPO NAME / EMAIL]

Key Regulatory Authorities

Other State AGs: See respective state AG websites