MEDCOR PRIVACY POLICY

www.medcor.com

Updated February 20, 2026

Medcor, Inc. ("Medcor", "we", "our" or "us") respects your privacy, and we are committed to protecting the security of information collected, processed, used, and stored in any format when visiting our Website, www.medcor.com including any (sub)pages associated with that domain ("Website"), our mobile application ("Mobile App"), and interactions with us offline ("Services"). We take reasonable measures to ensure that the personal information you give us is handled in a safe and responsible manner.

Medcor is the data controller (i.e. the entity that controls the collection and use of your information) in relation to any personal information that Medcor collects, uses, stores, or otherwise processes about you and is responsible for ensuring that such processing complies with applicable data protection laws, including information handled by our service providers.

This Privacy Policy ("Policy") covers personal information collected for non-HIPAA purposes (e.g., online interactions via the Website and offline interactions including customer service, marketing, recruitment, or non-clinical services). "Personal information" means information that identifies you or can reasonably be linked to you. This Policy describes the specific personal information Medcor may collect, how Medcor collects, uses, and shares your personal information and the choices you have regarding our use of your personal information.

This Policy does not cover our policies relating to personal health information (PHI). PHI is a subset of personal information that includes information that can identify you and that says something about your health, care, or payment for care—when a HIPAA-covered entity (or their vendor) has it. When we process PHI, HIPAA governs. When we process personal information outside HIPAA, state consumer privacy laws apply. If both could apply, HIPAA controls for PHI. To the extent you are or have been a patient at one of our clinics, we have a separate Privacy Policy that governs those interactions. You can access our Healthcare Privacy Policy **here**.

Our Website is not intended for users under the age of 16. We do not knowingly collect personal information from users under the age of 16. If you believe that a user under the age of 16 may have disclosed personal information to us, please refer to the **"How to contact us"** section.

Third Party Link Disclaimer: We are not responsible for the data policies or procedures for any third-party sites linked on our Website and this Policy does not cover such items.

Personal Information We Collect

While you are not required to provide personal information on the public areas of our Website or Mobile App, or when interacting with us via our Services, you may choose to voluntarily submit information through certain features, such as employment or business-related inquiries. If you do so, we may collect, use, and retain the information you provide in accordance with this Policy.

Additionally, we may collect the following categories of personal information from you in the course of business, including through your use of our Website or Mobile App, when you contact or request information from us, or otherwise engage in our Services:

Visitors to our Website

- **Identity Data:** information that tells us who you are including your first and last name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, unique device or user ID, email address telephone number.
- **Contact Data:** information that tells us how we can communicate with you including your e-mail address and telephone number.
- **Service Preferences Data:** information that tells us the Services you are interested in.
- **Professional Data:** information that indicates the company you work for, your job title and company contact information.
- **Geolocation Data:** data about the location of your device(s).
- **Technical Data:** information automatically collected from a browser, app, or device when you visit or use our Website or Mobile that is reasonably linked to you. It typically includes: IP address (and approximate location inferred from it, e.g., city/region), cookie IDs and other unique identifiers (e.g., mobile advertising ID, session ID), device and browser details (device type, OS, app version, browser type/version, language, screen resolution), network and connection information (carrier, connection type), log and event data (URLs requested, referrer/exit pages, timestamps, page loads, clicks/scrolls, feature use), diagnostics/performance and crash data, and security signals (authentication events, access attempts). We treat Technical Data as personal information when it is maintained or used in identifiable form; we maintain de-identified or aggregated data as de-identified.
- **Usage Data:** information that shows us how you interacted with our Website or Mobile App, such as referring website address, content and pages you accessed on our Website or Mobile App, clicks, and other actions taken on the Website or Mobile App.

Customers and Potential Customers

In addition to the above categories of Personal Information, we may also collect the following from Prospective Customers (“Prospects”) and Customers:

- **Contact data:** you directly submit to us including title, company name, company email address, telephone number, and demographic information including city and state.
- **Customer Service data** including information you share with us regarding your preferences about our Services (e.g. information about clinic location, engagement, or other issues relevant to our provision of the Services).
- **Geolocation Data.** data about the location of your device(s).

Job Applicants

If you choose to submit an application, to apply for a job with us we may collect the following personal information:

- **Identity data:** full name, address, telephone number, electronic email address, or other information necessary for job application process.
- **Education data**: educational history (e.g. institution name, year of graduation, degree obtained, GPA).
- **Employment data:** employment history (e.g. prior place of employment, duration of employment, job title and description of duties).
- **Sensitive Personal Information (SPI):** race, ethnicity or place of origin, veteran status, and disability status.

To the extent applicable, Medcor provides job applicants with the ability to limit the use of their SPI at the time of collection.

Employees or Contractors

In addition to the above categories of information, we may collect additional categories of SPI during the new hire screening and onboarding process and solely for legitimate employment-related purposes, including pre-employment background check information, drug and alcohol test results, vaccination/TB status, disability/medical accommodation information, payroll, benefits administration, and other information necessary for compliance with legal and regulatory obligations and workplace safety.

- **Identity data**: gender, photograph, employee identification number, and emergency contact information.
- **Sensitive Personal Information (SPI):** bank account and routing number, date of birth, gender, social security number, driver's license, state identification card, or passport number, citizenship or immigration status, and health data. Sensitive information also includes inferences drawn from your personal information relating to any of the sensitive personal information characteristics.

To the extent applicable, Medcor provides employees and contractors with the ability to limit the use of their SPI at the time of collection.

Categories of Data Collected in the Past 12 Months

In the preceding 12 months, the types of personal information Medcor has collected about California residents is reflected in the lists above.

How We Collect Personal Information

We collect most personal information directly from you in person, by telephone, text, or email, and/or via our Website, Mobile App or the Services. A detailed list of all sources for collection of personal information follow below:

Visitors to Our Website or Mobile App

- **Directly From You** including when you visit our Website or Mobile App, or otherwise interact with our Services, including account creation for our Client Portal, fill out a form, contact customer service or help lines including chatbots;
- **Affiliates.** Our corporate family may provide account/usage and support information for operational purposes.
- **Referral sources and partners.** Channel partners, event organizers, or referral programs that send us lead details.
- **Service Providers** such as our Website or Mobile App hosts, technology security vendor, analytics and diagnostic providers, survey host, and/or virtual helpdesk or chatbot.
- **Automatic collection from your browser/device.** Cookies, SDKs, pixels, log files, and similar technologies on our Website or Mobile App. See our **Cookie Policy** for more information about our Cookies and website tracking technologies);
- **Advertising & measurement partners (CCBA).** We receive ad interaction events, device/identifier data, attribution and conversion metrics, and audience-segment membership **related to our ads** on our Services or third-party sites/apps; these flows are subject to your **Do Not Sell or Share** choices and recognized opt-out signals.

Customers or Potential Customers

In addition to the above, which may apply if you use our Website or Mobile App, we may collect personal information from the following sources:

- **Directly from you during in-person interactions:** events or trade shows, onsite consultations, deliveries, installations, maintenance visits or other in-person interactions relating to our Services.
- **Call center and phone support:** inbound/outbound calls, SMS helplines, IVR, and call recordings/metadata (with notice). See our **Healthcare Privacy Policy**.
- **Security & facilities:** CCTV/video, access-control/visitor logs, reception sign-ins, parking validation systems (post signage where required).
- **Referrals & co-marketing:** referrals from customers or partners; co-branded events or lead shares from distributors/resellers.
- **Affiliates/corporate group:** intra-group sharing for centralized operations, analytics, or support.
- **Commercial sources:** list licensors, direct-mail cooperatives, demographic/propensity appends, address hygiene (e.g., NCOA), and verification services.

Job Applicants

In addition to the above, which may apply if you use our Website or Mobile App, we may collect personal information from the following sources:

- **Directly from the applicant:** applications, resumes/CVs, cover letters, assessments, or interviews.
- **Recruiting platforms & staffing agencies:** job boards, recruiters, RPOs, campus programs.
- **Professional references & former employers:** reference checks; employment/education verification.
- **Background check providers**

- **Licensing/credentialing bodies & educational institutions:** degrees, licenses, disciplinary status.
- **Pre-employment medical/drug testing providers:** post-offer only, ADA/GINA-compliant

Employees and Contractors

In addition to the above, which may apply if you use our Website or Mobile App, we may collect personal information from the following sources:

- **Directly from you**: HRIS entries, self-service portals, benefits elections, performance inputs, (contact information, emergency contact, beneficiary).
- **Time, scheduling & attendance systems**: badge swipes, timesheets, PTO, leave administration.
- **Payroll/benefits/retirement administrators & brokers**: compensation, tax, health/plan data.
- **Financial institutions** only with your consent for the purpose of facilitating payment of job compensation (e.g., your bank).
- **Device/IT systems & security tools:** corporate email, endpoint/MDM logs, SSO, IAM, security monitoring.
- **Facilities & EHS**: visitor logs, access control, CCTV, incident/safety reports.
- **Travel/expense & fleet/telemetry vendors**: itineraries, receipts, mileage, vehicle telematics.
- **Workers' compensation/insurers/TPAs**: claims administration.
- **Hotlines & investigations**: ethics/whistleblower systems, compliance vendors.
- **Occupational or other health providers**: fitness-for-duty, accommodations, vaccination/TB where applicable;

Why We Collect and Process Information

We may use your personal information for the following business purposes:

Provide the Services You Request

- **Visitors/Customers/Prospects:** Communicate about our Services and perform our contract or take steps at your request before entering into a contract.

Facilitate Our Website and Service Delivery

- **Visitors/Customers/Prospects:** Maintain/serve accounts; provide support (including chat/helpdesk); process or fulfill orders/transactions; verify customer information; process payments/financing; provide analytics/diagnostics and storage; and similar services performed on our behalf.
- **Job Applicants:** Operate applicant portals, scheduling, and candidate communications used for recruiting.

Account / Relationship Management

- **Visitors/Customers/Prospects:** customer relationship management, onboarding, renewals, and billing administration.

Improving Our Services

- **Visitors/Customers/Prospects:** Operational improvements such as efficiency, training, quality control, and customer service enhancements.
- **Job Applicants:** Improve the recruiting experience and candidate communications.
- **Employees/Contractors:** Improve internal tools, workflows, and employee support.

Business Intelligence and Data Audits

- **Visitors/Customers/Prospects:** Auditing (e.g., counting ad impressions, verifying positioning/quality), compliance with specifications/standards, business analyses and projections, and internal research for technological development/demonstration.
- **Job Applicants:** Audit and analyze recruiting systems and hiring outcomes.
- **Employees/Contractors:** Audit workforce systems/processes and support operational planning.

Communication Preferences

- **Visitors/Customers/Prospects:** Use contact details and limited interaction data (e.g., form submissions, site interactions, email engagement) to understand preferred channels/topics, tailor outreach, and measure effectiveness. (You may opt out of marketing at any time.)

Website and Data Security (Security & Debugging)

- **Visitors/Customers/Prospects:** Protect sites/systems; prevent, detect, investigate, and respond to fraud or malicious activity; debug/repair errors; authenticate users/manage access; safeguard our assets.
- **Job Applicants:** Secure recruiting systems; prevent abuse and unauthorized access.
- **Employees/Contractors:** Secure enterprise systems, facilities, and devices; access control and incident response.

Marketing or Advertising

- **Visitors/Customers/Prospects:** Market our Services (updates, invitations, and non-personalized on-site messages during your current visit) and tailor messages based on your interactions; service providers deliver these communications under contracts that limit their use of personal information. You can opt out of marketing at any time. We may also deliver and measure ads for our Services across non-affiliated sites and apps (cross-context behavioral advertising); you may opt out of sale/sharing, and we honor recognized opt-out signals.

De-Identified / Aggregated Analytics

- **Visitors/Customers/Prospects:** Create and use de-identified or aggregated data for analytics, reporting, and business insights.
- **Job Applicants:** Create and use de-identified or aggregated recruiting analytics.
- **Employees/Contractors:** Create and use de-identified or aggregated HR analytics. (We maintain de-identified data as de-identified.)

Corporate Transactions

- **Visitors/Customers/Prospects:** Use/disclosure as reasonably necessary for mergers, acquisitions, financings, or asset sales with appropriate safeguards.
- **Job Applicants:** Inclusion of recruiting records as reasonably necessary for diligence and transition planning.
- **Employees/Contractors:** Inclusion of workforce records as reasonably necessary for diligence and transition planning.

Fulfill Legal Requirements (Compliance & Legal Disputes)

- **Visitors/Customers/Prospects:** Gather/provide information required by or relating to audits, inquiries, or investigations by regulatory bodies; respond to lawful requests; and maintain related compliance records.
- **Job Applicants:** For the same reasons listed in the "Visitor/Customer/Prospects" category and expanded to include the additional business purpose for recruiting-related records.
- **Employees/Contractors:** For the same reasons listed in the "Visitor/Customer/Prospects" category and expanded to include additional business purposes, including employment, tax, benefits, safety, and workplace reporting; contract enforcement and defense of legal claims.

Job Recruitment and Hiring

- **Job Applicants:** Screen, identify, and evaluate candidates; manage interview logistics and communications; maintain hiring records; analyze hiring processes and outcomes; and conduct background checks where permitted by applicable law (and subject to any local recruitment privacy policy).

HR Operations

- **Employees/Contractors:** Administer payroll, tax, and benefits; manage time, attendance, and leave; operate IT and facilities (including access control and security monitoring); provide training and performance management; and support health/safety and workers' compensation.

With Your Consent (all consumers): For any additional purposes we describe at the time of collection, where we obtain your consent when required.

How We May Disclose Information

We will not disclose your personal information to third parties other than as described in this Policy unless we have your permission or are required or permitted to do so by law. We may share such information with our affiliates as necessary to carry out the purposes for which the information was supplied or collected. Similarly, third party contractors, consultants and/or vendors engaged by Medcor to provide Services may have access to your personal information. These third parties will be subject to their own data protection requirements providing the same or greater level of security provided by Medcor and in most instances will also have entered into a written agreement with us which addresses access to and use of your personal information.

We may disclose your personal information to the below categories of third parties for the stated business purposes:

Affiliates (Medcor entities)

- **Visitors/Prospects/Customers**: To operate and support our Website and Services; respond to inquiries; coordinate account or relationship management.
- **Applicants/Employees/Contractors**: To administer recruiting, onboarding, HR, payroll, benefits, IT, and compliance functions across our corporate group.

Service Providers and Vendors

- **Visitors/Prospects/Customers:** To host our Website or Mobile App; provide services to customers and/or customer support (including chat/virtual helpdesk); process payments and financing; perform analytics/diagnostics; survey administration; IT, security, and professional services (e.g., auditors, legal counsel).
- **Applicants/Employees/Contractors:** To support recruiting platforms, background screening, scheduling and communications, HRIS/payroll/benefits administration, IT and facilities operations, security monitoring, training, and professional services.

Regulators, Government, and Law Enforcement

- **Visitors/Prospects/Customers:** To comply with laws and regulations; respond to lawful requests, subpoenas, court orders, and regulatory inquiries.
- **Applicants/Employees/Contractors:** For the same reasons disclosed above and expanded to include additional legal obligations, including employment, tax, benefits, safety, and workplace reporting obligations**.**

Security and Protection of Rights

- **Visitors/Prospects/Customers:** To protect our Services and users; prevent, detect, investigate, and respond to fraud, unauthorized access, or misuse; enforce our Terms of Use; and address threats to health, safety, or legal rights.
- **Applicants/Employees/Contractors:** For the same reasons disclosed above and expanded to include additional reasons for disclosure, including workplace security, incident response, internal investigations, and protection of company assets.

Corporate Transactions (M&A/Financings)

- **Visitors/Prospects/Customers**: As reasonably necessary to evaluate or complete a merger, acquisition, financing, asset sale, restructuring, bankruptcy/insolvency, or similar transaction (including due diligence with lenders, auditors, attorneys, and consultants).
- **Applicants/Employees/Contractors:** For the same reasons disclosed above and expanded to include additional reasons for disclosure, including workforce-related diligence and transition of HR records consistent with applicable law.

Aggregate and Deidentified Recipients

- **Visitors/Prospects/Customers**: We may share deidentified or aggregated information (not reasonably capable of being linked to an individual) with partners, service providers, or publicly—for example, to analyze trends, improve services, or publish research and reports.

- **Applicants/Employees/Contractors**: For the same reasons disclosed above and expanded to include additional reasons for disclosure including for HR analytics, planning, training, reporting, or research—maintained and disclosed in deidentified/aggregated form.

Other Disclosures (all consumer categories): In ways we notify you of at the time and, where required, obtain your consent.

Disclosures for a business purpose in the preceding 12 months
In the preceding 12 months, Medcor has disclosed the above listed categories of personal information to its service providers for the specific, limited business purposes as described.

Security

We have implemented technical and organizational security measures in an effort to safeguard the personal information in our custody and control. Such measures include, for example, limiting access to personal information only to staff and authorized service providers on a need-to-know basis for the purposes described in this Policy, as well as other administrative, technical, and physical safeguards.

We endeavor to take all reasonable steps to protect your personal information, but cannot guarantee the security of any data you disclose online. Please note that email is not a secure medium and should not be used to send confidential or sensitive information. By providing information online, you accept the inherent security risks of providing information over the Internet and will not hold us responsible for any breach of security, unless it is due to our negligence or willful default.

Data Transfer

Medcor is comprised of multiple offices and affiliated entities in numerous jurisdictions. Details regarding our offices and certain of our affiliated entities can be found on our Website **Medcor.com**. Your personal information may be transferred to or shared across our integrated computer networks with one or more of Medcor's offices and our affiliated offices in the United States and other countries that may not be subject to data protection laws similar to those prevailing in the jurisdiction in which such information is provided to or received by us. However, all of our offices adhere to the same procedures with respect to your personal information, including this Policy.

Data Retention

Your personal information is only stored and retained for as long as necessary for the purposes set out in this Policy. In determining the appropriate retention period, we consider the nature and duration of our relationship with you, the type of services provided, and the impact on our services if certain information is deleted. You can access information about how long cookie data is retained by us in our **Cookie Policy**. In all cases, Medcor may retain personal information for additional time as required by applicable law; to establish, exercise or defend our legal rights; or, for other legitimate business purposes, including archiving and historical purposes. We will maintain such data in an anonymized form where practical.

Your Rights

Depending on your jurisdiction and subject to certain limitations, you may have the following rights with respect to the personal information we process about you:

- **Right to know** what personal information we have collected about you, including:
    - The categories of personal information we have collected;
    - The categories of sources from which the personal information is collected;
    - The business or commercial purpose for collecting, selling, or sharing personal information;
    - The categories of third parties to whom we disclose personal information; and
    - The specific pieces of personal information we have collected about you.

- **Right to delete** personal information that we have collected from you with certain exceptions, including where the information is necessary to facilitate our ongoing provision of Services to you. Subject to the exceptions set out below, on receipt of a verifiable request from you, we will:
    - Delete your personal information from our records;
    - Direct any service providers or contractors to delete your personal information from their records;
    - Direct third parties to whom the business has sold or shared your personal information to delete your personal information unless this proves impossible or involves disproportionate effort (in which case we will provide you with a detailed explanation).

    Please note that we may not delete your personal information if it is reasonably necessary to:
    - Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by you, or reasonably anticipated within the context of our ongoing business relationship with you, or otherwise perform a contract between you and us;
    - Help to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for those purposes;
    - Debug to identify and repair errors that impair existing intended functionality;
    - Exercise free speech, ensure the right of another consumer to exercise their right of free speech, or exercise another right provided for by law;
    - Comply with the California Electronic Communications Privacy Act;
    - Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when our deletion of the information is likely to render impossible or seriously impair the achievement of such research, provided we have obtained your informed consent;
    - Enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us;
    - Comply with an existing legal obligation; or
    - Otherwise use your personal information, internally, in a lawful manner that is compatible with the context in which you provided the information.

- **Right to correct inaccurate personal information that we maintain about you.** Upon receipt of a verifiable request from you, we will use commercially reasonable efforts to correct the inaccurate personal information.

- **Right to opt-out of the sale or sharing** of your personal information for cross-contextual behavioral advertising.

- **Right not to receive discriminatory treatment** for exercising any of these rights. This means we cannot, among other things:
    - Deny goods or services to you;
    - Charge different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
    - Provide a different level or quality of goods or services to you; or
    - Suggest that you will receive a different price or rate for goods or services or a different level or quality of goods or services.

Exercising Your Rights

To exercise your rights as set out above, please contact us using our contact details described in the **"How to contact us"** section, indicating the type of right you would like to exercise and that you are making the request under an applicable U.S. state data privacy law.

In order to process your deletion and/or access request, we are permitted by law to collect certain information about you to verify your identity. If, however, we cannot verify your identity from the information already maintained by us, we may request additional information from you, which shall only be used for the purposes of verifying your identity, and for security or fraud-prevention purposes, such as a passport or driver's license.

Under the laws of your state, you may have the right to use an authorized agent to submit a request on your behalf if you provide the authorized agent written permission signed by you. We may also require that you verify (as consumer) verify your identity directly with us and confirm that you have provided the authorized agent permission to act on their behalf.

We will make every effort to respond to your request within 45 days from when you contacted us. If you have a complex request, the law may permit us to take longer to respond. We will still contact you within 45 days from when you contacted us to let you know we need more time.

If we decline to take action on a request that you have submitted, we will inform you of our reasons for doing so and provide instructions for how to appeal the decision. Depending on your state of residence you may have the right to appeal within a reasonable period of time after you have received our decision. If you have this appeal right, within 45-60 days, depending on the state, of our receipt of your appeal, we will inform you in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If we deny your appeal, we will provide you with a method for contacting your state attorney general's office to submit a complaint.

Do Not Sell or Share My Personal Information

You have the right to opt out of the sale or sharing of your personal information for purposes of cross-contextual behavior advertising or targeted advertising under the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA), and certain other privacy and data protection laws, as applicable. You can do so **here** or by clicking the **Do Not Sell or Share** link at the bottom of our landing page.

We honor “opt-out preference signals,” such as the Global Privacy Control (GPC). When your browser sends a valid GPC signal, we treat it as a request to opt out of “selling” or “sharing” your personal information for cross-context behavioral advertising. We apply this choice to the browser or device that sends the signal and, if you are logged in or otherwise identifiable, we also apply it to your account (including across our offline activities where applicable). You don’t need to submit a separate request, create an account, or click any additional buttons, and we won’t charge you or degrade your experience

because of this choice (you may simply see fewer personalized ads). If you use multiple browsers or devices, enable GPC on each to carry your preference everywhere.

California “Shine the Light” Notice

If you are a California resident, you may request information about our compliance with the Shine the Light law by contacting us in the following ways: emailing privacy@medcor.com or by calling our toll-free compliance number (866) 709-9507. Please note that the CCPA and Shine the Light are different laws offering different rights and requests must be made separately.

Do Not Track

Please note that we do not support “Do Not Track” browser settings at this time. DNT is different from opt-out preference signals required by California law. (We continue to honor GPC/opt-out preference signals as described above.)

How to Contact Us

Questions, concerns, or requests regarding Medcor’s Privacy Policy or practices should be directed to:

- Medcor, Inc. at **privacy@medcor.com**
- Toll-free compliance number (866) 709-9507 (during normal business hours, Monday through Friday, except public holidays)
- Submitting a form here via the Website’s **"Contact Us" page**

Disclaimer:
While every attempt has been made to create/establish policies consistent with federal, state, and local law, if an inconsistency arises, this Policy will be enforced consistent with the applicable law. Medcor reserves the right to modify, amend, or terminate this policy at its sole discretion and in accordance with applicable laws.