PRIVACY POLICY

Judith Ruth Enterprise Corporation

Effective Date: April 18, 2026

Last Updated: April 18, 2026

Founder & CEO: Natalie McCall-Gaston, FNP-BC

Headquarters: Douglasville, Georgia

TABLE OF CONTENTS

1. INTRODUCTION AND SCOPE

1.1 Who We Are. Judith Ruth Enterprise Corporation, doing business as Judith Ruth Medical Center ("Company," "we," "us," or "our"), is a healthcare and telehealth organization founded by Natalie McCall-Gaston, FNP-BC, and headquartered in Douglasville, Georgia. We provide medical, telehealth, and wellness services to patients and consumers across multiple states.

1.2 Purpose. This Privacy Policy describes how Judith Ruth Enterprise Corporation collects, uses, discloses, retains, and protects your personal information and protected health information when you interact with us. It also explains your rights regarding your information and how you may exercise those rights.

1.3 Scope. This Privacy Policy applies to all individuals who access or use our websites, mobile applications, telehealth platforms, patient portals, electronic health record systems, and any other digital or in-person services operated or provided by Judith Ruth Enterprise Corporation or Judith Ruth Medical Center. This includes, without limitation:

(a) Patients and prospective patients;

(b) Visitors to our websites and digital properties;

(c) Users of our telehealth platforms and patient portals;

(d) Individuals who communicate with us via email, telephone, or other channels;

(e) Job applicants and employees to the extent set forth herein; and

(f) Third parties who interact with our services on behalf of patients.

1.4 Geographic Applicability. Judith Ruth Enterprise Corporation operates across multiple states, including Georgia, New Mexico, Nevada, Vermont, Connecticut, New York, and Washington. This Privacy Policy is designed to comply with the privacy and data protection laws applicable in each state in which we operate. Where state-specific requirements apply, they are identified in the relevant sections of this Policy.

1.5 Agreement. By accessing or using any of our services, you acknowledge that you have read, understood, and agree to the collection, use, and disclosure of your information as described in this Privacy Policy. If you do not agree with the practices described herein, please do not use our services.

2. DEFINITIONS

For the purposes of this Privacy Policy, the following terms shall have the meanings set forth below:

2.1 "Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal Information does not include publicly available information, deidentified or aggregated consumer information, or information excluded from the scope of applicable privacy laws.

2.2 "Protected Health Information" or "PHI" means individually identifiable health information, as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 45 C.F.R. §160.103, that is created, received, maintained, or transmitted by Judith Ruth Enterprise Corporation in its capacity as a Covered Entity. PHI includes information relating to the past, present, or future physical or mental health condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.

2.3 "Sensitive Personal Information" means Personal Information that reveals a consumer's Social Security number, driver's license number, state identification card number, passport number, account log-in credentials, financial account information, precise geolocation, racial or ethnic origin, religious beliefs, union membership, personal communications content,

genetic data, biometric information processed for identification purposes, health information, or information concerning a consumer's sex life or sexual orientation.

2.4 **"Service Provider"** means a person or entity that processes Personal Information on behalf of Judith Ruth Enterprise Corporation pursuant to a written contract that prohibits the entity from retaining, using, or disclosing the Personal Information for any purpose other than the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the Personal Information for a commercial purpose other than providing the contracted services.

2.5 **"Business Purpose"** means the use of Personal Information for the Company's operational purposes, or other notified purposes, provided that the use of Personal Information is reasonably necessary and proportionate to achieve the operational purpose for which it was collected or processed, or for another operational purpose that is compatible with the context in which the Personal Information was collected.

2.6 **"Commercial Purpose"** means the advancement of a person's commercial or economic interests, such as inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

2.7 **"Consumer"** means a natural person who is a resident of a state in which Judith Ruth Enterprise Corporation operates and whose Personal Information is collected, used, or disclosed by the Company, whether in the individual's capacity as a patient, website visitor, or otherwise.

2.8 **"Household"** means a group of consumers who cohabitate at the same residential address and share use of common devices or services.

2.9 **"Device"** means any physical object that is capable of connecting to the Internet, directly or indirectly, or to another Device, including but not limited to desktop computers, laptops, smartphones, tablets, and wearable health devices.

2.10 **"Sale"** means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by

electronic or other means, a Consumer's Personal Information by the Company to a third party for monetary or other valuable consideration.

2.11 **"Sharing"** means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a Consumer's Personal Information by the Company to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

2.12 **"Telehealth Services"** means the delivery of healthcare services, including medical consultations, diagnoses, treatment recommendations, prescription services, and follow-up care, conducted remotely through telecommunications technology, including video conferencing, telephone, secure messaging, and other electronic means, as provided by Judith Ruth Medical Center.

2.13 **"Covered Entity"** means a health plan, a healthcare clearinghouse, or a healthcare provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA. Judith Ruth Enterprise Corporation, operating as Judith Ruth Medical Center, is a Covered Entity under HIPAA.

2.14 **"Business Associate"** means a person or entity that performs certain functions or activities on behalf of, or provides certain services to, a Covered Entity that involve the use or disclosure of Protected Health Information, as defined under 45 C.F.R. §160.103.

3. INFORMATION WE COLLECT

3.1 **Categories of Personal Information.** Judith Ruth Enterprise Corporation may collect the following categories of Personal Information, depending on the nature of your interaction with us:

Category	Examples
Identifiers	Real name, alias, postal address, email address, telephone number, date of birth, Social Security number (where required), insurance identification number, medical record number, account name, IP address, or other similar identifiers.

Category	Examples
Commercial Information	Records of services obtained, purchasing or consuming histories, and payment records related to healthcare services, products, or subscriptions.
Internet/Network Activity	Browsing history on our websites, search history, information regarding interactions with our websites, applications, patient portals, or telehealth platforms, including clickstream data and session recordings.
Geolocation Data	Approximate location derived from IP address; precise geolocation only when explicitly authorized by the user for service delivery or emergency purposes.
Biometric Information	Physiological data collected through connected health devices or telehealth platforms where applicable, including vitals monitoring data, with your express consent.
Professional/Employment Information	Current or past employer, job title, and professional information provided by job applicants or as relevant to healthcare services (e.g., occupational health assessments).
Education Information	Education records to the extent relevant to employment applications or patient intake processes.
Inferences	Inferences drawn from any of the above categories to create a profile reflecting preferences, characteristics, health trends, behavior, or attitudes.
Sensitive Personal Information	Social Security number, driver's license or state identification number, account log-in credentials, precise geolocation, racial or ethnic origin, health information, genetic data, and biometric data used for identification.

3.2 Sources of Information. We collect Personal Information from the following sources:

(a) **Directly from you** — when you register for an account, schedule an appointment, complete patient intake forms, submit inquiries, subscribe to communications, or otherwise provide information to us;

(b) **Automatically** — when you access or use our websites, applications, or telehealth platforms, through cookies, web beacons, pixels, log files, and similar technologies;

(c) **From third parties** — including healthcare analytics providers, identity verification services, marketing partners, public databases, and social media platforms (where applicable);

(d) **From healthcare providers** — including referring physicians, specialists, laboratories, pharmacies, and other healthcare entities involved in your care; and

(e) **From insurance and payer sources** — including health insurance companies, managed care organizations, Medicare, Medicaid, and other third-party payers for purposes of coverage verification, claims processing, and coordination of benefits.

3.3 Health and Medical Information. Through Judith Ruth Medical Center's telehealth services and in-person care, we collect health and medical information including, but not limited to: medical history, current symptoms, diagnoses, treatment plans, prescription information, laboratory and diagnostic test results, imaging records, allergies, immunization records, mental and behavioral health information, and provider notes. This information constitutes Protected Health Information under HIPAA and is subject to additional protections as described in Section 12 of this Policy.

3.4 Device and Technical Information. When you use our digital services, we automatically collect technical information about your Device, including: Device type and model, operating system and version, browser type and version, screen resolution, language preferences, unique device identifiers, mobile advertising identifiers, network connection type, referring URLs, and pages viewed. For telehealth sessions, we may also collect information about your audio/video hardware capabilities and network connection quality to ensure service delivery.

4. HOW WE USE YOUR INFORMATION

4.1 Providing and Improving Services. We use your Personal Information to operate, maintain, and improve our healthcare services, websites, mobile

applications, telehealth platforms, and patient portals. This includes creating and managing your accounts, authenticating your identity, processing your requests, and personalizing your experience with Judith Ruth Medical Center.

4.2 Telehealth Service Delivery. We use your information to facilitate telehealth consultations, including scheduling virtual appointments, establishing secure video and audio connections, transmitting clinical information between you and your provider, and ensuring the technical functionality of our telehealth platform.

4.3 Treatment, Payment, and Healthcare Operations. We use your Protected Health Information for treatment purposes (providing, coordinating, and managing your healthcare), payment purposes (billing, claims management, insurance verification, collections, and utilization review), and healthcare operations (quality assessment, competency assurance, conducting or arranging for medical review, and business planning and development).

4.4 Communication and Appointment Scheduling. We use your information to communicate with you regarding your appointments, treatment plans, prescription refills, follow-up care, appointment reminders, and other service-related notifications. We may contact you via email, text message, telephone, secure messaging through the patient portal, or postal mail.

4.5 Billing and Insurance Processing. We use your information to submit claims to your health insurance plan, process copayments, deductibles, and coinsurance, verify insurance eligibility and benefits, manage patient accounts, process payments, and pursue collections for outstanding balances in accordance with applicable law.

4.6 Analytics and Service Improvement. We use aggregated and de-identified information to analyze usage patterns, measure the effectiveness of our services, identify areas for improvement, conduct research and statistical analysis, and develop new services and features.

4.7 Legal Compliance and Regulatory Obligations. We use your information to comply with applicable federal, state, and local laws, regulations, and legal processes, including HIPAA, state telehealth laws, reporting obligations, and responding to lawful requests from public authorities.

4.8 **Marketing.** With your consent or as otherwise permitted by law, we may use your information to send you marketing communications about health-related services, wellness programs, and other offerings of Judith Ruth Medical Center. You have the right to opt out of marketing communications at any time by following the unsubscribe instructions included in each communication, adjusting your account preferences, or contacting us at privacy@judithruthmedical.com. Please note that even after opting out of marketing, you will continue to receive transactional and service-related communications.

4.9 **Fraud Prevention and Security.** We use your information to detect, investigate, and prevent fraudulent transactions, unauthorized access, and other illegal activities, and to protect the rights, property, and safety of Judith Ruth Enterprise Corporation, our patients, and others.

5. HOW WE SHARE YOUR INFORMATION

5.1 **Service Providers and Business Associates.** We share your information with third-party service providers and Business Associates who perform services on our behalf, including but not limited to: electronic health record system providers, telehealth platform operators, cloud hosting providers, IT security firms, billing and coding services, appointment scheduling platforms, email and communication service providers, and analytics providers. All such parties are contractually required to protect your information and to use it only for the purposes for which it was disclosed. Business Associates handling PHI are bound by Business Associate Agreements as required under HIPAA.

5.2 **Treatment, Payment, and Healthcare Operations.** We may share your PHI with other healthcare providers involved in your treatment, with your health plan for payment purposes, and with entities assisting in our healthcare operations, as permitted under HIPAA.

5.3 **Payment Processors.** We share payment-related information with third-party payment processors to facilitate transactions. Please refer to Section 11 of this Privacy Policy for detailed information about our payment processor

relationships, including Apple Pay, Google Pay, Stripe, and other payment services.

5.4 **Insurance Companies and Payers.** We share your information with health insurance companies, managed care organizations, government healthcare programs (including Medicare and Medicaid), and other third-party payers for purposes of claims submission, eligibility verification, prior authorization, coordination of benefits, and other payment-related activities.

5.5 **As Required by Law.** We may disclose your information when required to do so by federal, state, or local law, regulation, subpoena, court order, or other legal process. This includes disclosures to public health authorities, regulatory agencies, law enforcement, and government agencies as mandated by applicable law.

5.6 **Business Transfers.** In the event of a merger, acquisition, reorganization, bankruptcy, asset sale, or other business transfer involving Judith Ruth Enterprise Corporation, your information may be transferred to the acquiring entity or successor. We will provide notice of any such transfer and any choices you may have regarding your information.

5.7 **With Your Consent.** We may share your information with third parties when you have provided your express consent or at your direction. For certain uses of PHI not described in this Policy, we will obtain your written authorization before using or disclosing your information.

5.8 **De-Identified or Aggregated Data.** We may share de-identified or aggregated data that cannot reasonably be used to identify you with third parties for research, analytics, public health, or other lawful purposes. De-identification is performed in accordance with the standards set forth in 45 C.F.R. §164.514.

6. COOKIES AND TRACKING TECHNOLOGIES

6.1 **Types of Cookies.** Our websites and digital services use cookies and similar tracking technologies. Cookies are small data files placed on your Device when you visit our websites. We use the following types of cookies:

(a) **Essential Cookies:** Required for the operation of our websites and patient portal. These cookies enable core functionality such as security, account authentication, and session management. They cannot be disabled.

(b) **Functional Cookies:** Enable enhanced functionality and personalization, such as remembering your preferences, language settings, and login information.

(c) **Analytics Cookies:** Collect information about how visitors use our websites, including which pages are visited most often, how visitors navigate between pages, and whether error messages are displayed. These cookies help us improve website performance.

(d) **Advertising Cookies:** Used to deliver advertisements relevant to you and your interests. They are also used to limit the number of times you see an advertisement and to help measure the effectiveness of advertising campaigns. We do not use advertising cookies to target healthcare-related advertisements based on your health information.

6.2 Cookies Policy. For comprehensive information about the specific cookies we use, their purposes, durations, and providers, please refer to our separate Cookies Policy, available on our website.

6.3 Managing Cookie Preferences. You may manage your cookie preferences through the cookie consent banner displayed on our website, through your browser settings, or by contacting us. Most web browsers allow you to control cookies through their settings, including accepting, rejecting, or deleting cookies. Please note that disabling certain cookies may affect the functionality of our websites and patient portal.

6.4 Third-Party Analytics. We use third-party analytics services, including Google Analytics, to help analyze how users interact with our websites. These services use cookies and similar technologies to collect and analyze usage information. Google Analytics collects information such as how often users visit our website, which pages they visit, and which other sites they visited prior to coming to our website. We use this information solely to improve our websites and services. You may opt out of Google Analytics by installing the Google Analytics Opt-Out Browser Add-on.

7. YOUR PRIVACY RIGHTS

7.1 General Rights. Depending on your state of residence and the applicable laws, you may have the following rights with respect to your Personal Information:

(a) **Right to Access:** You have the right to request that we disclose the categories and specific pieces of Personal Information we have collected about you.

(b) **Right to Correction:** You have the right to request that we correct inaccurate Personal Information we maintain about you.

(c) **Right to Deletion:** You have the right to request that we delete Personal Information we have collected from you, subject to certain exceptions provided by law.

(d) **Right to Data Portability:** You have the right to request a copy of your Personal Information in a structured, commonly used, and machine-readable format.

(e) **Right to Opt-Out:** You have the right to opt out of the sale or sharing of your Personal Information, as applicable.

7.2 How to Exercise Your Rights. You may submit a verifiable consumer request to exercise your privacy rights by contacting us through the following methods:

(a) Email: privacy@judithruthmedical.com

(b) Submitting a request through the privacy rights web form on our website

(c) Calling our privacy line (number provided on our website)

7.3 Verification Process. Upon receiving your request, we will take reasonable steps to verify your identity before responding. The verification process may require you to provide information that matches information we already have on file, such as your name, email address, date of birth, or account information. For requests to access specific pieces of Personal Information or to delete Personal Information, we apply a heightened verification standard. We may ask you to provide a signed declaration under penalty of perjury that you are the Consumer whose Personal Information is the subject of the request.

7.4 Authorized Agents. You may designate an authorized agent to submit a request on your behalf. If you use an authorized agent, we may require the agent to provide proof of written authorization or a valid power of attorney. We may also require the Consumer to directly verify their own identity with us and confirm that they authorized the agent to act on their behalf.

7.5 Non-Discrimination. Judith Ruth Enterprise Corporation will not discriminate against you for exercising any of your privacy rights. We will not deny you services, charge you different prices or rates, provide a different level or quality of services, or suggest that you will receive a different price, rate, or quality of services because you exercised a privacy right.

7.6 Response Timeframes. We will acknowledge receipt of your request within ten (10) business days. We will respond to your verifiable consumer request within forty-five (45) calendar days of receiving it. If we require additional time, we will inform you of the reason and extension period in writing. We may extend the response period by an additional forty-five (45) calendar days when reasonably necessary, provided we notify you within the initial 45-day period.

8. CALIFORNIA PRIVACY RIGHTS — CCPA/CPRA

This section applies to California residents and supplements the information in this Privacy Policy with disclosures required under the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "CCPA").

8.1 Right to Know / Right to Access. California residents have the right to request that we disclose: (a) the categories of Personal Information we have collected; (b) the categories of sources from which Personal Information was collected; (c) the business or commercial purpose for collecting, selling, or sharing Personal Information; (d) the categories of third parties to whom we disclose Personal Information; and (e) the specific pieces of Personal Information we have collected about the Consumer.

8.2 Right to Delete. California residents have the right to request deletion of Personal Information that we have collected from them, subject to exceptions under Cal. Civ. Code §1798.105(d), including where retention is necessary to complete a transaction, comply with a legal obligation, detect security incidents, exercise free speech, conduct research in the public interest, or enable solely internal uses reasonably aligned with the consumer's expectations.

8.3 Right to Correct. California residents have the right to request that we correct inaccurate Personal Information that we maintain about them, taking into account the nature of the Personal Information and the purposes of the processing.

8.4 Right to Opt-Out of Sale or Sharing. California residents have the right to opt out of the sale of their Personal Information and the sharing of their Personal Information for cross-context behavioral advertising. To exercise this right, you may submit a request via our "Do Not Sell or Share My Personal Information" link on our website, by emailing privacy@judithruthmedical.com, or by calling our toll-free number. We will process opt-out requests within fifteen (15) business days.

8.5 Right to Limit Use of Sensitive Personal Information. California residents have the right to limit our use and disclosure of their Sensitive Personal Information to uses that are necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those services or goods, and to uses authorized by applicable regulations. We primarily use Sensitive Personal Information for purposes of healthcare delivery, which is necessary to provide our services.

8.6 Right to Non-Discrimination. We will not discriminate against California residents for exercising any of the rights described in this section, including by denying services, charging different prices or rates, providing a different level or quality of services, or suggesting that the consumer will receive a different price or rate or a different level or quality of services.

8.7 Categories of Personal Information — Disclosure Table. The following table describes the categories of Personal Information we have collected, disclosed for a business purpose, sold, or shared in the preceding twelve (12) months:

Category of PI	Collected	Disclosed for Business Purpose	Sold	Shared	Categories of Recipients
Identifiers (name, address, email, phone, etc.)	Yes	Yes	No	No	Service providers, healthcare providers, payers
Personal Information under Cal. Civ. Code §1798.80(e)	Yes	Yes	No	No	Service providers, payers, payment processors
Protected Classification Characteristics	Yes	Yes	No	No	Service providers, healthcare providers
Commercial Information	Yes	Yes	No	No	Service providers, payment processors
Biometric Information	Yes (limited)	Yes	No	No	Service providers, healthcare providers
Internet/ Network Activity	Yes	Yes	No	No	Analytics providers, service providers
Geolocation Data	Yes	Yes	No	No	Service providers
Professional/ Employment Information	Yes	Yes	No	No	Service providers
Education Information	Yes (limited)	No	No	No	N/A
Inferences	Yes	No	No	No	N/A
Sensitive Personal Information	Yes	Yes	No	No	Service providers, healthcare providers, payers

8.8 Financial Incentives. Judith Ruth Enterprise Corporation does not offer financial incentives, price differences, or service differences to consumers in exchange for the retention, sale, or sharing of Personal Information. If we offer any such program in the future, we will provide a separate notice describing the material terms of the program, including the categories of Personal Information involved and the value of your data.

8.9 Data Retention Periods. We retain each category of Personal Information only for as long as reasonably necessary for the purposes disclosed in this Policy. Specific retention periods are set forth in Section 15 of this Privacy Policy. Where a specific retention period is not designated, we retain data for the shorter of (a) the period reasonably necessary for the business purpose for which it was collected, or (b) the applicable statute of limitations period.

8.10 Metrics Disclosure. As required by CCPA regulations, Judith Ruth Enterprise Corporation will compile and disclose the following metrics for the preceding calendar year, to be published annually on or before July 1: (a) the number of requests to know received, complied with (in whole or in part), and denied; (b) the number of requests to delete received, complied with (in whole or in part), and denied; (c) the number of requests to opt-out received, complied with (in whole or in part), and denied; and (d) the median number of days within which we substantively responded to each category of request.

8.11 How to Submit CCPA Requests. California residents may submit CCPA requests through the following methods:

(a) **Email:** privacy@judithruthmedical.com

(b) **Toll-Free Telephone Number:** Available on our website

(c) **Web Form:** Accessible through the "Privacy Rights" or "Do Not Sell or Share My Personal Information" links on our website

8.12 Authorized Agent Procedures. A California resident may use an authorized agent to submit a request to know, delete, or opt-out on their behalf. If an authorized agent submits a request, we may require: (a) written permission signed by the Consumer authorizing the agent to make the request; (b) verification of the agent's identity; and (c) direct verification from the Consumer that they authorized the agent. These requirements do not apply when an agent provides a valid power of attorney under California Probate Code §§4000–4465.

8.13 Automated Decision-Making Technology (ADMT). In compliance with CCPA regulations effective in 2026, Judith Ruth Enterprise Corporation discloses the following: We may use automated decision-making technology in limited contexts, such as fraud detection and appointment scheduling optimization. We do not use ADMT to make decisions that produce legal effects or effects of similar significance concerning a consumer without human involvement. Where ADMT is used, consumers have the right to: (a) receive information about the logic involved and the intended output of the ADMT; (b) opt out of the use of ADMT in decisions that produce significant effects; and (c) request access to information about the ADMT and how it was used in connection with their Personal Information. Requests related to ADMT may be submitted to privacy@judithruthmedical.com.

8.14 CCPA Inquiries. For all inquiries related to the CCPA or your California privacy rights, please contact us at privacy@judithruthmedical.com.

9. CALIFORNIA SHINE THE LIGHT (CAL. CIV. CODE §1798.83)

9.1 Your Rights Under Shine the Light. Under California's "Shine the Light" law (Cal. Civ. Code §1798.83), California residents who have an established business relationship with Judith Ruth Enterprise Corporation may request information about whether we have disclosed Personal Information to any third parties for the third parties' direct marketing purposes during the preceding calendar year.

9.2 Information Available Upon Request. If applicable, the information provided will include: (a) a list of the categories of Personal Information disclosed to third parties for the third parties' direct marketing purposes during the immediately preceding calendar year; and (b) the names and addresses of all such third parties.

9.3 How to Make a Shine the Light Request. To make a request under the Shine the Light law, please send a written request to us by email at privacy@judithruthmedical.com or by postal mail to our address set forth in Section 20. Please include "California Shine the Light Request" in the subject

line or on the envelope, and provide your name and the email address and/or mailing address associated with your account.

9.4 Response Procedures and Timeframes. We will respond to Shine the Light requests within thirty (30) days of receipt. Our response will cover the one-year period preceding the request.

9.5 Annual Request Limitation. Please note that we are required to respond to one request per California customer each year pursuant to Cal. Civ. Code §1798.83. We do not charge a fee for responding to Shine the Light requests.

10. DO NOT TRACK DISCLOSURE

10.1 Do Not Track Signals. "Do Not Track" ("DNT") is a privacy preference that you can set in certain web browsers. When you turn on DNT, the browser sends a signal to websites requesting that your browsing activity not be tracked. At this time, there is no universally accepted standard for how companies should respond to DNT signals. Judith Ruth Enterprise Corporation currently does not alter our data collection and use practices in response to DNT signals from your browser.

10.2 Global Privacy Control (GPC). We honor Global Privacy Control ("GPC") signals as a valid opt-out of sale/sharing request under the California Consumer Privacy Act. When we detect a GPC signal from your browser, we will treat it as a request to opt out of the sale or sharing of Personal Information associated with that browser. The GPC signal applies to the specific browser and device from which it is sent.

10.3 Browser-Based Opt-Out Mechanisms. In addition to GPC, you may use your browser settings to manage cookies and tracking technologies as described in Section 6. You may also use industry opt-out tools such as the Digital Advertising Alliance's opt-out page or the Network Advertising Initiative's opt-out page to manage interest-based advertising.

10.4 Interaction with Data Collection. While we do not currently respond to browser-based DNT signals, our treatment of GPC signals, combined with our cookie management tools and opt-out mechanisms described elsewhere in this Policy, provide you with meaningful control over how your data is collected and used across our digital services.

11. PAYMENT PROCESSOR DISCLOSURES

11.1 Overview. Judith Ruth Enterprise Corporation uses third-party payment processors to handle financial transactions for services provided by Judith Ruth Medical Center. We do not store full payment card numbers, card verification values (CVV), or complete bank account numbers on our servers. Payment information is transmitted directly to and processed by our payment processor partners using industry-standard encryption and tokenization.

11.2 Apple Pay. When you make a payment using Apple Pay, your actual credit or debit card number is not stored on your device or on our servers. Instead, Apple assigns a unique Device Account Number, which is encrypted and securely stored in the Secure Element of your device. We receive a transaction-specific dynamic security code, a sanitized transaction confirmation, and limited payment details (such as the last four digits of your card number and transaction amount). Apple's privacy practices govern the data Apple collects and retains. For more information, please refer to Apple's Privacy Policy.

11.3 Google Pay. When you make a payment through Google Pay, Google tokenizes your payment credentials and transmits them to our payment processor. We receive transaction confirmation details, including a transaction reference number, the amount charged, and limited card information. We do not receive or store your full card number. Google's privacy practices govern the data Google collects and retains in connection with Google Pay. For more information, please refer to Google's Privacy Policy.

11.4 Stripe. Judith Ruth Enterprise Corporation uses Stripe, Inc. as a primary payment processor. Stripe is certified as a PCI-DSS Level 1 Service Provider, the highest level of certification in the payment card industry. Stripe collects and processes payment card information, billing addresses, and related transaction data. Stripe acts as a data processor on our behalf and is contractually bound to process data only as instructed by us and in accordance with applicable data protection laws. Where Stripe Connect is utilized for sub-merchant or multi-party transactions, Stripe may collect

additional information as required for its regulatory and compliance obligations. For more information, please refer to Stripe's Privacy Policy.

11.5 Other Payment Methods. We may also accept payments through the following methods, each governed by their respective privacy policies:

(a) **PayPal:** When you pay via PayPal, your financial information is processed and stored by PayPal. We receive transaction confirmations and limited account information. Please refer to PayPal's Privacy Policy for details.

(b) **Credit/Debit Card Processors:** Traditional credit and debit card payments are processed through our PCI-DSS compliant payment infrastructure. Card data is encrypted in transit and tokenized at the point of capture.

(c) **HSA/FSA Card Processors:** We accept Health Savings Account (HSA) and Flexible Spending Account (FSA) cards for eligible healthcare expenses. These transactions are processed through our standard payment infrastructure with appropriate merchant category codes to facilitate automatic eligibility verification.

11.6 PCI-DSS Compliance. Judith Ruth Enterprise Corporation maintains compliance with the Payment Card Industry Data Security Standard (PCI-DSS). We undergo regular assessments to validate our compliance and employ industry-standard security controls to protect payment data.

11.7 Insurance and Copayment Processing. When we process insurance claims, copayments, deductibles, or coinsurance, we transmit relevant billing information (including procedure codes, diagnosis codes, and patient demographic information) to your health plan through secure electronic data interchange (EDI) channels in compliance with HIPAA transaction standards.

11.8 Payment Data Security. All payment data transmitted between your Device and our systems, and between our systems and our payment processors, is encrypted using Transport Layer Security (TLS) 1.2 or higher. Payment card data is tokenized so that sensitive card information is replaced with a non-sensitive equivalent (token) that cannot be used outside the specific transaction context.

11.9 Payment Processor Privacy Policies. We encourage you to review the privacy policies of our payment processors. We are not responsible for the privacy practices of third-party payment processors. Links to their respective privacy policies are available on our website.

12. HIPAA AND HEALTH INFORMATION

12.1 HIPAA Compliance. Judith Ruth Enterprise Corporation, operating as Judith Ruth Medical Center, is a Covered Entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations, including the HIPAA Privacy Rule (45 C.F.R. Parts 160 and 164, Subparts A and E), the HIPAA Security Rule (45 C.F.R. Parts 160 and 164, Subparts A and C), and the HIPAA Breach Notification Rule (45 C.F.R. Parts 160 and 164, Subpart D). We are committed to protecting the privacy and security of your Protected Health Information in compliance with all applicable HIPAA requirements.

12.2 Notice of Privacy Practices. In addition to this Privacy Policy, Judith Ruth Medical Center maintains a separate Notice of Privacy Practices ("NPP") as required by HIPAA. The NPP describes in detail how we may use and disclose your PHI, your rights with respect to your PHI, and our legal obligations regarding your PHI. A copy of the NPP is provided to all patients and is available upon request and on our website.

12.3 How PHI Is Protected. We implement comprehensive administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of your PHI. These safeguards include encryption of PHI at rest and in transit, role-based access controls, workforce training, audit logging and monitoring, secure disposal procedures, and regular risk assessments. Our electronic health record systems meet or exceed applicable certification standards.

12.4 Patient Rights Under HIPAA. As a patient of Judith Ruth Medical Center, you have the following rights under HIPAA with respect to your PHI:

(a) **Right of Access:** You have the right to inspect and obtain a copy of your PHI maintained in a designated record set, subject to limited exceptions. We will provide the information in the form and format you request if it is readily producible, or in a mutually agreeable format.

(b) **Right to Amend:** You have the right to request an amendment to your PHI in a designated record set if you believe the information is incorrect or incomplete. We may deny the request under certain circumstances as specified by HIPAA.

(c) **Right to an Accounting of Disclosures:** You have the right to request a list of certain disclosures of your PHI made by us during the six (6) years prior to the date of your request.

(d) **Right to Request Restrictions:** You have the right to request that we restrict certain uses and disclosures of your PHI. We are not required to agree to all restriction requests, except that we must agree to restrict disclosures to a health plan for payment or healthcare operations purposes when you have paid for the service in full out of pocket.

(e) **Right to Confidential Communications:** You have the right to request that we communicate with you about your health information by alternative means or at alternative locations.

(f) **Right to Complain:** You have the right to file a complaint with us or with the Secretary of the U.S. Department of Health and Human Services if you believe your privacy rights have been violated. We will not retaliate against you for filing a complaint.

12.5 Relationship Between This Privacy Policy and the NPP. This Privacy Policy governs the collection and use of Personal Information (including non-health information) across all of our digital and in-person services. Our Notice of Privacy Practices specifically governs the use and disclosure of Protected Health Information as required by HIPAA. Where PHI is concerned, the NPP controls to the extent of any conflict with this Privacy Policy. We encourage you to review both documents.

12.6 Business Associate Agreements. We require all Business Associates who access, receive, maintain, or transmit PHI on our behalf to enter into Business Associate Agreements ("BAAs") in compliance with 45 C.F.R. §164.502(e) and §164.504(e). These agreements require Business Associates to implement appropriate safeguards to protect PHI, report security incidents and breaches, and comply with applicable HIPAA requirements.

12.7 Telehealth-Specific Data Protections. PHI transmitted during telehealth sessions is protected through end-to-end encryption, secure video conferencing platforms that have been evaluated for HIPAA compliance, and

BAAs with telehealth technology providers. Telehealth session recordings, if any, are stored in encrypted form in HIPAA-compliant data centers and are subject to the same access controls and retention policies as other PHI.

13. TELEHEALTH AND MULTI-STATE COMPLIANCE

13.1 State-Specific Telehealth Privacy Requirements. Judith Ruth Medical Center provides telehealth services in multiple states, each with its own privacy and data protection requirements. The following summarizes key state-specific requirements:

State	Key Telehealth Privacy Requirements
Georgia (GA)	Georgia law requires informed consent for telehealth services. Providers must comply with state medical record retention requirements (minimum ten years for adults, age of majority plus five years for minors). Patient data collected through telemedicine must be secured in accordance with applicable state and federal law.
New Mexico (NM)	New Mexico requires that telehealth providers obtain informed consent prior to delivering services and that patients be informed of their right to refuse telehealth. Providers must comply with New Mexico's medical records privacy provisions and maintain records in accordance with state licensing board requirements.
Nevada (NV)	Nevada law requires specific informed consent disclosures for telehealth services, including the right to refuse telehealth. Nevada also has data privacy provisions under NRS Chapter 603A requiring businesses to implement reasonable security measures and provide breach notification. Medical records must be retained for a minimum of five years.
Vermont (VT)	Vermont requires informed consent for telemedicine and imposes obligations regarding the security of electronic health records. Vermont's data broker regulations (9 V.S.A. Chapter 62) and health privacy

State	Key Telehealth Privacy Requirements
	protections may apply to certain data collection activities. Medical records must be retained according to Vermont Board of Medical Practice requirements.
Connecticut (CT)	The Connecticut Data Privacy Act (CTDPA) provides consumers with rights including the right to access, correct, delete, obtain a copy of, and opt out of processing of their personal data. Connecticut requires informed consent for telehealth and mandates compliance with state medical records retention requirements (minimum seven years).
New York (NY)	New York's SHIELD Act (N.Y. Gen. Bus. Law §899-aa) requires businesses to implement reasonable safeguards to protect private information of New York residents. Telehealth services must comply with New York Education Law and Public Health Law. Medical records must be retained for a minimum of six years (or three years after the patient reaches age 21 for minors).
Washington (WA)	The Washington My Health My Data Act (Chapter 19.373 RCW) provides comprehensive protections for consumer health data, including consent requirements for collection and sharing, the right to access and delete health data, and geofencing prohibitions around healthcare facilities. Washington also requires informed consent for telemedicine under RCW 70.41.020. Medical records must be retained for a minimum of ten years.

13.2 Informed Consent for Telehealth. Before providing telehealth services, Judith Ruth Medical Center obtains informed consent from each patient. The informed consent process includes disclosure of: (a) the nature and scope of the proposed telehealth services; (b) the risks, benefits, and alternatives to telehealth; (c) the patient's right to refuse telehealth and to request an in-person visit; (d) the potential for technology failures during the session; (e) how patient data will be collected, used, stored, and protected; and (f) any applicable state-specific disclosures.

13.3 Recording and Storage of Telehealth Sessions. Judith Ruth Medical Center does not routinely record audio or video of telehealth sessions. If a

telehealth session is to be recorded for any purpose (such as quality assurance or training), we will obtain your express written consent prior to recording. Clinical notes and documentation generated during telehealth sessions are stored in our electronic health record system in encrypted form and are subject to the same privacy and security protections as all other medical records.

13.4 Cross-State Data Transfer Protections. When providing telehealth services to patients located in a state other than Georgia, Judith Ruth Enterprise Corporation ensures that data transfers between states comply with the privacy and security requirements of both the state in which the patient is located and the state in which our servers and staff are located. All cross-state data transfers are conducted over encrypted channels and are governed by our internal data governance policies.

13.5 State-Specific Consumer Privacy Rights. In addition to rights available under the CCPA (Section 8), consumers in the following states have additional privacy rights:

(a) **Connecticut (CTDPA):** Right to access, correct, delete, obtain a portable copy of personal data, and opt out of processing for targeted advertising, sale, or profiling. We will respond to requests within 45 days. Consumers may appeal a denial within a reasonable period.

(b) **New York (SHIELD Act):** Right to reasonable data security safeguards. The SHIELD Act requires us to implement administrative, technical, and physical safeguards for the private information of New York residents.

(c) **Washington (My Health My Data Act):** Right to consent to collection and sharing of consumer health data, right to access collected health data, right to delete consumer health data, right to withdraw consent at any time. We are prohibited from geofencing healthcare facilities for the purpose of collecting consumer health data or identifying or tracking consumers seeking healthcare services.

14. DATA SECURITY

14.1 Administrative Safeguards. Judith Ruth Enterprise Corporation maintains comprehensive administrative safeguards, including: designated

privacy and security officers responsible for the development and implementation of policies and procedures; workforce privacy and security training conducted upon hiring and annually thereafter; documented policies and procedures governing the use, disclosure, and protection of Personal Information and PHI; sanctions policies for workforce members who violate privacy or security policies; and regular risk assessments to identify and mitigate vulnerabilities.

14.2 Technical Safeguards. We implement technical safeguards, including: encryption of data at rest using AES-256 or equivalent encryption standards; encryption of data in transit using TLS 1.2 or higher; firewalls and intrusion detection/prevention systems; secure system configuration and patch management; anti-malware and endpoint protection; audit logging and monitoring of system access and activity; and secure backup and disaster recovery systems.

14.3 Physical Safeguards. We maintain physical safeguards, including: facility access controls limiting physical access to areas where Personal Information and PHI are stored or processed; workstation security policies governing the placement and use of workstations that access sensitive data; device and media controls governing the receipt, removal, transfer, and disposal of electronic media and hardware containing data; and secure disposal of physical records containing Personal Information or PHI.

14.4 Access Controls and Authentication. Access to Personal Information and PHI is restricted to authorized workforce members and Business Associates who require access to perform their job duties or contracted services. We implement role-based access controls, unique user identification, automatic session timeouts, and multi-factor authentication for access to systems containing sensitive data.

14.5 Employee Training. All workforce members receive privacy and security training upon hire and at least annually thereafter. Training covers: HIPAA privacy and security requirements; recognition and reporting of potential security incidents and breaches; proper handling and disposal of PHI and Personal Information; phishing and social engineering awareness; and acceptable use of information systems.

14.6 Incident Response. Judith Ruth Enterprise Corporation maintains a documented incident response plan that provides procedures for identifying, containing, investigating, and remediating security incidents. Our incident response team includes designated privacy and security personnel and is supported by external forensic and legal resources as needed.

14.7 Breach Notification. In the event of a breach of unsecured PHI, we will notify affected individuals, the Secretary of the U.S. Department of Health and Human Services, and (for breaches affecting 500 or more individuals in a state or jurisdiction) prominent media outlets, in compliance with the HIPAA Breach Notification Rule (45 C.F.R. §§164.400–414). We will provide notification without unreasonable delay and in no event later than sixty (60) calendar days from the date of discovery of the breach. For breaches of Personal Information subject to state breach notification laws (including, without limitation, the laws of Georgia, New York, Connecticut, Nevada, New Mexico, Vermont, and Washington), we will comply with the notification timelines and requirements established by each applicable state statute.

15. DATA RETENTION

15.1 Retention Periods by Data Category. We retain Personal Information and PHI for the periods described below, unless a longer retention period is required by applicable law:

Data Category	Retention Period	Basis
Medical Records (Adult Patients)	10 years from last encounter (or longer per applicable state law)	State medical records retention laws; HIPAA
Medical Records (Minor Patients)	Until age of majority plus applicable state retention period (varies by state)	State medical records retention laws
Billing and Insurance Records	7 years from date of service	Tax and regulatory requirements; payer contracts
Account and Registration Data	Duration of active account plus 3 years	Business need; legal compliance
Telehealth Session Documentation	Same as Medical Records	State and federal medical records requirements

Data Category	Retention Period	Basis
Payment Transaction Records	7 years from transaction date	Tax, PCI-DSS, and regulatory requirements
Website Analytics and Cookies Data	26 months from collection	Analytics platform default; business need
Marketing and Communications Preferences	Duration of active relationship plus 3 years	CAN-SPAM; business need
Employment Application Data	3 years from application date	Equal employment opportunity compliance
Incident and Complaint Records	6 years from resolution	HIPAA; legal compliance
Business Associate Agreement Records	6 years from termination of agreement	HIPAA §164.530(j)

15.2 Medical Records Retention by State. Where we provide services to patients in multiple states, we retain medical records for the longer of the retention period required by the state in which the patient received services or the state in which the patient resides, or Georgia's retention requirements (as our home state), whichever is longest.

15.3 Criteria for Determining Retention Periods. In determining the appropriate retention period for Personal Information and PHI, we consider: (a) the nature and sensitivity of the data; (b) the purposes for which it was collected; (c) applicable legal, regulatory, and contractual obligations; (d) applicable statutes of limitations; (e) the potential risk of harm from unauthorized use or disclosure; and (f) our legitimate business needs.

15.4 Secure Disposal. When Personal Information or PHI is no longer required to be retained, we dispose of it in a secure manner designed to prevent unauthorized access, use, or disclosure. Electronic records are permanently deleted using industry-standard data sanitization methods (e.g., cryptographic erasure, secure overwrite). Physical records are cross-cut shredded or incinerated. Media containing sensitive data is degaussed or physically destroyed prior to disposal.

16. CHILDREN'S PRIVACY

16.1 COPPA Compliance. Judith Ruth Enterprise Corporation complies with the Children's Online Privacy Protection Act ("COPPA"). Our websites, applications, and online services are not directed to children under the age of thirteen (13), and we do not knowingly collect Personal Information from children under the age of 13 through our online services.

16.2 No Knowing Collection from Children. If we become aware that we have collected Personal Information from a child under the age of 13 without verified parental consent, we will take steps to delete such information promptly. If you believe that we have inadvertently collected Personal Information from a child under 13, please contact us immediately at privacy@judithruthmedical.com.

16.3 Parental Rights. Parents and legal guardians have the right to: (a) review the Personal Information we have collected from their child; (b) request deletion of such information; and (c) refuse to allow further collection or use of their child's information. To exercise these rights, parents may contact us using the methods described in Section 20.

16.4 Minor Patient Data Under HIPAA. When Judith Ruth Medical Center provides healthcare services to minors, medical information collected in the course of treatment is Protected Health Information under HIPAA and is handled in accordance with HIPAA requirements and applicable state laws governing minors' health information. Access to a minor's PHI by parents or guardians is governed by state law and HIPAA regulations at 45 C.F.R. §164.502(g).

17. INTERNATIONAL DATA TRANSFERS

17.1 Data Processed in the United States. Judith Ruth Enterprise Corporation is headquartered in Douglasville, Georgia, and our services are primarily directed to individuals located in the United States. Your Personal

Information and PHI are processed and stored on servers located within the United States.

17.2 No Routine International Transfers. We do not routinely transfer Personal Information or PHI outside of the United States. If any transfer of data outside the United States becomes necessary (for example, in connection with a service provider located outside the U.S.), we will disclose such transfers in an update to this Privacy Policy and implement appropriate safeguards, including contractual protections, to ensure your data receives an adequate level of protection.

17.3 Transfer Mechanisms. In the event that international data transfers become necessary, we will rely on applicable transfer mechanisms, which may include standard contractual clauses, consent, or other lawful bases as required under applicable law, to ensure that your Personal Information receives a level of protection consistent with that provided under U.S. law.

18. THIRD-PARTY LINKS AND SERVICES

18.1 Third-Party Websites and Services. Our websites and digital services may contain links to websites, applications, or services operated by third parties that are not under the control of Judith Ruth Enterprise Corporation. These links are provided for your convenience and informational purposes only.

18.2 No Responsibility for Third-Party Practices. Judith Ruth Enterprise Corporation is not responsible for the privacy practices, data collection policies, content, or security of third-party websites or services. The inclusion of a link on our website does not imply endorsement of the linked website or any association with its operators.

18.3 Review Third-Party Policies. We strongly encourage you to review the privacy policy and terms of use of any third-party website or service before providing any Personal Information. Your interactions with third-party websites and services are governed solely by the policies and terms of those third parties.

19. CHANGES TO THIS PRIVACY POLICY

19.1 Right to Update. Judith Ruth Enterprise Corporation reserves the right to modify, amend, or update this Privacy Policy at any time and at our sole discretion. We will update the "Last Updated" date at the top of this Policy to reflect the date of any changes.

19.2 Notification of Material Changes. If we make material changes to this Privacy Policy that affect your rights or the way we collect, use, or share your Personal Information, we will notify you by: (a) posting a prominent notice on our website; (b) sending an email to the address associated with your account (if applicable); (c) providing a notification through our patient portal or mobile application; or (d) other means as required by applicable law. Material changes will be identified as such in the notification.

19.3 Continued Use. Your continued use of our services following the posting of changes to this Privacy Policy constitutes your acceptance of such changes. If you do not agree with a revised Privacy Policy, you should discontinue use of our services and contact us to close your account and request deletion of your data, subject to our legal obligations to retain certain information.

19.4 Archive of Prior Versions. Archived versions of prior Privacy Policies are available upon request. To obtain a copy of a previous version of this Privacy Policy, please contact us at privacy@judithruthmedical.com and identify the approximate date or version you are requesting.

20. CONTACT INFORMATION

20.1 General Inquiries. If you have any questions, concerns, or comments regarding this Privacy Policy or our privacy practices, please contact us at:

Judith Ruth Enterprise Corporation

Attn: Privacy Office

Douglasville, GA 30135

Email: privacy@judithruthmedical.com

Phone: [To Be Provided]

20.2 Data Protection Inquiries. For questions specifically related to the protection, use, or disclosure of your Personal Information or Protected Health Information, including requests to exercise your privacy rights, please direct your inquiry to our Privacy Office at the address or email listed above.

20.3 CCPA-Specific Contact Methods. California residents may submit CCPA requests through the following channels:

(a) Email: privacy@judithruthmedical.com (subject line: "CCPA Request")

(b) Toll-Free Telephone Number: Available on our website

(c) Online Web Form: Accessible via the "Privacy Rights" link on our website

20.4 Complaints and Regulatory Contacts. If you believe that your privacy rights have been violated, you may file a complaint with Judith Ruth Enterprise Corporation's Privacy Office at the contact information above. You also have the right to file a complaint with the following regulatory bodies:

(a) **U.S. Department of Health and Human Services, Office for Civil Rights:** For complaints related to HIPAA violations involving your Protected Health Information.

(b) **California Attorney General:** For complaints related to CCPA/CPRA violations involving your Personal Information as a California resident.

(c) **State Attorneys General:** For privacy complaints under state consumer protection laws in Georgia, New Mexico, Nevada, Vermont, Connecticut, New York, or Washington.

(d) **Federal Trade Commission (FTC):** For complaints related to unfair or deceptive data practices.

We will not retaliate against you for filing a complaint in good faith with any regulatory authority.

ACKNOWLEDGMENT

By using the services of Judith Ruth Enterprise Corporation and Judith Ruth Medical Center, you acknowledge that you have read, understood, and agree to the terms and practices described in this Privacy Policy. This Privacy Policy is effective as of April 18, 2026. If you have questions or concerns, please contact

our Privacy Office at privacy@judithruthmedical.com.