

Política de Privacidad del Paciente de Sana - Versión en Español

Fecha de vigencia: 10 de agosto de 2025

Bienvenido/a a **Sana** ("Sana", «nosotros», «nuestro» o «la Compañía»). Su confianza es esencial para nuestro éxito; por ello protegemos rigurosamente la información de salud y los datos personales de quienes utilizan nuestra plataforma y servicios de telesalud (los «Servicios»). Al acceder o utilizar los Servicios, usted reconoce haber leído y aceptado esta Política y los Términos y Condiciones de Sana, que se incorporan por referencia.

1. Alcance

Esta Política describe cómo recopilamos, usamos, compartimos y protegemos la Información Personal y la Información de Salud Protegida («PHI», por sus siglas en inglés) de pacientes y usuarias de Sana. No se aplica a empresas o personas que no controlamos ni gestionamos directamente.

2. Bases legales y reglamentarias

- **Legislación federal:** HIPAA (1996) y sus reglamentos de implementación; HITECH Act (2009); Regla de Notificación de Brechas de la FTC (2024).
- **Legislación estatal de privacidad:** Sana cumple con todas las leyes de privacidad vigentes en los estados donde presta servicios — incluidas, sin limitarse a Texas y Florida — así como en cualquier otra jurisdicción en la que ofrezcamos los Servicios. Sana cumple con HIPAA y las disposiciones de Texas HB 300.
- **Leyes escudo de salud reproductiva** aplicables.

Puede presentar quejas ante la **FTC** o ante la oficina del **Fiscal General** de su estado. En caso de conflicto entre leyes, Sana aplicará la que otorgue mayor protección al paciente.

3. Aviso de Prácticas de Privacidad (NPP) HIPAA

Como *covered entity* (entidad cubierta), Sana entrega un Aviso que detalla (i) usos y divulgaciones permitidos de PHI, (ii) deberes de protección y notificación, (iii) sus derechos, (iv)

cómo quejarse ante la OCR/AG, y (v) fecha de vigencia. El aviso está en su panel y en la sección «Legal» de la página web.

4. Cambios a esta Política

Publicaremos versiones actualizadas en **sanamujer.com** y notificaremos cambios materiales con un mínimo de 30 días de antelación. El uso continuado implica aceptación.

5. Notificación de brechas de seguridad

Si ocurre una brecha de PHI o datos personales no asegurados, se le notificará con un máximo de 60 días calendario desde su descubrimiento, según HIPAA y la FTC.

6. Información que recopilamos

6.1 Información que usted nos proporciona

- Identificadores personales.
- Documentos de identidad y **fotografías clínicas** (no se usan para reconocimiento facial ni se comparten con fines biométricos conforme a BIPA/CUBI).
- Información médica y de salud.
- Información de seguros y facturación.
- Comunicaciones en la plataforma.

Usted no nos va a proporcionar credenciales de autenticación directamente, sino a Carepatron, nuestro sistema de EHR. No analizamos ni almacenamos características biométricas de la voz.

6.2 Información recopilada automáticamente

- IP, identificadores de dispositivo, navegador y SO.
- Geolocalización aproximada.

No se usarán cookies ni ninguna tecnología parecida.

6.3 Información de terceros

- Datos de proveedores, laboratorios, farmacias, aseguradoras o PBM.
- Datos de socios de analítica y marketing (prevención de fraude).

6.4 Tabla «Categoría – Finalidad – Retención – Terceros» (exigida por la CPA)

Categoría (CPA § 6)	Finalidad principal	¿Se vende/Comparte?	Retención máxima
Identificadores personales	Crear cuenta, verificar identidad, envíos	No	10 años tras última interacción
PHI / Expediente clínico	Telesalud, diagnóstico, receta	No	≥ 10 años o el plazo legal estatal que sea mayor
Credenciales	Autenticación segura	No	Mientras exista la cuenta
Datos financieros	Cobro y reembolsos	No	7 años (requisitos IRS)
Geolocalización aproximada	Cumplimiento prescripción por estado	No	1 año
Datos técnicos	Seguridad, analítica	No	26 meses (p. ej., Google Analytics con enmascaramiento de IP)”

No vendemos ni compartimos datos con terceros para publicidad dirigida.

7. Cómo usamos su información

Finalidad	Ejemplos
Provisión de servicios	Crear/gestionar cuenta; consultas; pagos; recetas
Cumplimiento normativo	Verificar identidad; registros; reportes HIPAA/CPA
Mejora y personalización	Analizar uso; nuevas funciones; recordatorios
Comunicaciones	Notificaciones transaccionales; recordatorios
Marketing opcional	Promociones con su consentimiento
Seguridad	Detección de fraude

8. Sistemas automatizados e IA

Es posible que usemos IA para priorizar solicitudes y recordatorios. No se toman decisiones médicas o legales exclusivamente automatizadas. Evaluaciones de impacto disponibles (CO SB-205, 2026).

9. Compartir información

Solo compartimos datos según la ley: (i) proveedores, (ii) socios con BAA, (iii) fusiones, (iv) órdenes legales válidas, (v) datos agregados.

Aviso de incentivos financieros: no ofrecemos descuentos ni recompensas por sus datos.

Protección salud reproductiva: impugnaremos citaciones de otros estados.

10. Retención y destrucción de datos

Registros clínicos: mayor de **10 años** o plazo legal del estado donde se brindó el servicio.

Destrucción segura.

11. Cookies, rastreo y No rastrear (“Do Not Track”)

No usamos cookies esenciales/funcionales/analíticas; bloqueamos píxeles que envíen PHI.

Honramos señales **Global Privacy Control** y «Do Not Track».

12. Seguridad de la información

Salvaguardas administrativas, técnicas y físicas; respuesta a incidentes según la Sección 5.

Los datos en tránsito están protegidos con cifrado de extremo a extremo TLS 1.3; los datos en reposo se cifran con AES-256. El acceso a la información de salud protegida (PHI) requiere autenticación multifactor, permisos basados en roles y bloqueo automático de pantalla tras cinco (5) minutos de inactividad. Los registros de auditoría rastrean todo acceso y cambio; dichos registros se conservan durante seis años. Aunque Sana emplea salvaguardas de estándar industrial, ningún sistema es completamente seguro. Una vulneración o acceso no autorizado, aunque improbable, sigue siendo un riesgo potencial.

13. Derechos bajo HIPAA y leyes estatales de privacidad vigentes

- **Acceso y portabilidad**
- **Corrección** de datos inexactos.
- **Eliminación** (derecho al olvido, salvo obligaciones legales).
- **Contabilidad de divulgaciones** (últimos 6 años, excl. TPO).
- **Exclusión de venta, publicidad dirigida y profiling** (según las leyes de su estado—p. ej., CPA, VCDPA, CTDPA, OCPA, TDPSA...).
 - Para ejercerlo, escriba a privacidad@sanamujer.com indicando «NO VENTA».
- **Limitación de datos sensibles** (CO CPA).
- **Apelación:** si denegamos su solicitud, podrá apelar en 45 días enviando «APELACIÓN» a privacidad@sanamujer.com. Decidiremos en 45 días; si se mantiene la denegación, puede quejarse ante el AG de su estado.
- **Representantes personales** (tutores, albaceas) pueden ejercer derechos en su nombre.

Cómo ejercer estos derechos

Envíe la solicitud vía portal seguro o email privacidad@sanamujer.com. Verificaremos identidad mediante (i) confirmación de correo y (ii) coincidencia de dos datos de registro (p. ej., fecha de nacimiento + número de teléfono). Si no logramos verificarle, le notificaremos y podrá aportar documentación adicional (ID con foto). Respondemos dentro de 30 días; una prórroga única de 30 días si es necesario. En Texas, responderemos a solicitudes de acceso a PHI dentro de 15 días hábiles (Tex. Health & Safety Code §181.103). Podrían aplicarse cargos razonables por copias. Si no logramos verificar su identidad, le indicaremos qué información adicional necesitamos o denegaremos la solicitud. Un agente autorizado deberá presentar carta notariada o poder simple más prueba de identidad del solicitante

Revocación de autorizaciones

Puede revocar consentimientos (p. ej., marketing) en cualquier momento mediante el portal o correo; no afecta usos previos.

14. Marketing y SMS (TCPA)

Al optar por SMS, otorga consentimiento expreso. Responda «STOP» para cancelar; «HELP» para ayuda. Tarifas podrían aplicar.

15. Datos reproductivos y leyes-escudo

No divulgaremos datos reproductivos fuera de su estado salvo orden federal válida y agotaremos recursos legales.

16. Menores

Servicios para mayores de 18 años; no recopilamos datos de menores de 13.

17. Accesibilidad y no discriminación (1557 ACA)

Política disponible en español/inglés; intérpretes y formatos accesibles sin coste; no discriminamos.

18. Servicios de terceros

Revise las políticas antes de proporcionar datos.

19. Grabación de audio/vídeo

No grabamos consultas salvo consentimiento; se cifran y eliminan a los 30 días. Cuando la ley estatal exija conservar grabaciones de telemedicina, Sana las almacenará de forma cifrada por el plazo mínimo legal aplicable.

20. Contacto

Oficial de Privacidad: Sergio D. Capdevila

Correo: privacidad@sanamujer.com

Tel.: 1-248-574-2623 (lun-vie, 6 a. m.–1 p. m. Hora Central CT)

Dirección: 5900 Balcones Dr STE 100, Austin, TX 78731

Última actualización: 10 de agosto de 2025

Sana Patient Privacy Policy - English Version

Effective Date: August 10, 2025

Welcome to **Sana** ("Sana," "we," "our," or "the Company"). Your trust is essential to our success; therefore, we rigorously safeguard the health information and personal data of everyone who uses our telehealth platform and services (the "Services"). By accessing or using the Services, you acknowledge that you have read and accept this Policy and Sana's Terms and Conditions, which are incorporated by reference.

1. Scope

This Policy describes how we collect, use, share, and protect Personal Information and Protected Health Information ("PHI") of Sana's patients and users. It does not apply to companies or individuals we do not control.

2. Legal & Regulatory Bases

- **Federal law:** HIPAA (1996) and its implementing regulations; HITECH Act (2009); FTC Health Breach Notification Rule (2024).
- **State privacy laws:** Sana complies with every state privacy statute in force where we operate — including, but not limited to, Texas and Florida — as well as any other jurisdiction in which our Services are offered. Sana complies with Texas HB 300 law as well.
- **Reproductive-health shield laws** where applicable.

You may also file privacy complaints with the **FTC** or with your state **Attorney General**. If there is a conflict between laws, Sana will apply the one that affords the greatest protection to the patient.

3. HIPAA Notice of Privacy Practices (NPP)

Sana's NPP covers permitted uses/disclosures, duties, individual rights, complaints (OCR/AG), and effective date. Available in your dashboard and the website in the legal section.

4. Changes to This Policy

Updates will post on **sanamujer.com**; material changes notified at least 30 days in advance.

5. Breach Notification

For unsecured PHI/personal-data breaches, Sana notifies you within 60 calendar days of discovery, per HIPAA & FTC.

6. Information We Collect

6.1 Information You Provide

- Personal identifiers.
- ID docs & **clinical photos** (not used for facial recognition or shared for biometric purposes per BIPA/CUBI).
- Medical & health info.
- Insurance/billing.
- In-platform communications.

You will not provide authentication credentials directly to us; instead, you will enter them in Carepatron, our EHR system. We do not analyze or store biometric voice characteristics.

6.2 Automatically Collected

- IP, device IDs, browser, OS.
- Approx. geolocation.

Cookies or similar technologies will not be used

6.3 From Third Parties

- Providers, labs, pharmacies, insurers, PBMs.
- Analytics/fraud-prevention partners.

6.4 "Category – Purpose – Retention – Third Parties" Table (CPA Rule 6)

Category	Primary Purpose	Sold/Shared ?	Max Retention
Personal identifiers	Account creation, identity verification, shipping	No	10 yrs after last interaction

PHI / Medical record	Telehealth, diagnosis, prescribing	No	≥ 10 yrs or state minimum, whichever is greater
Credentials	Secure authentication	No	While account active
Financial data	Billing/refunds	No	7 yrs (IRS)
Technical data	Security, analytics	No	26 months (Google Analytics with IP masking and filters to ensure that no PHI is transmitted.)
Approx. geolocation	State-compliance prescribing	No	1 year

We do **not** sell or share data for targeted advertising.

7. How We Use Your Information

Purpose	Examples
Service delivery	Manage account; telehealth visits; payments; prescriptions
Regulatory compliance	ID verification; HIPAA/CPA logs
Improvement & personalization	Usage analytics; features; reminders
Communications	Transactional notices; renewals
Optional marketing	Promotions with consent
Security	Fraud detection
Research	De-identified data (45 CFR §164.514(b))

8. Automated Systems & AI

It is possible that AI is used to help triage and provide appointment reminders. However, no medical or legal decision is made solely automatically. Impact assessments available (CO SB-205, 2026).

9. Information Sharing

We share only as law allows: providers, BAAs, business transfers, valid legal orders, de-identified data.

Financial-incentive notice: Sana offers **no** discounts/rewards for your data.

Reproductive-health protection: We challenge out-of-state subpoenas.

10. Data Retention & Destruction

Clinical records kept the longer of **10 years** or state minimum; securely destroyed.

11. Cookies, Tracking & "Do Not Track"

We don't use essential, functional & analytics cookies; We perform blocking on pixels that send PHI . We honor **Global Privacy Control** and "Do Not Track" browser signals.

12. Information Security

Administrative, technical & physical safeguards; incident response per Section 5. Data in transit is protected with TLS 1.3 end-to-end encryption; data at rest is encrypted with AES-256. Access to PHI requires multi-factor authentication, role-based permissions, and automatic screen-lock after 5 minutes of inactivity. Audit logs track all access and changes; logs are retained 6 years. Although Sana uses industry-standard safeguards, no system is entirely secure. A breach or unauthorized access, though unlikely, remains a potential risk.

13. Rights under HIPAA and Applicable State Privacy Laws

- **Access & portability**
- **Correction** of inaccurate data.
- **Deletion** (subject to legal retention).
- **Accounting of disclosures** (last 6 yrs, excl. TPO).
- **Opt out of sale, targeted ads, profiling** (according to your state laws p. ej., CPA, VCDPA, CTDPA, OCPA, TDPSA...)
 - To opt out, please email privacidad@sanamujer.com with the subject "DO NOT SELL".
- **Limit sensitive data** (CO CPA).
- **Appeal:** If we deny a request, email "APPEAL" within 45 days. We decide in 45 days; If unresolved, File with your AG.
- **Personal representatives** (guardians, executors) may act on your behalf.

Exercising These Rights

Submit requests via secure portal or **privacidad@sanamujer.com**. We verify identity with (i) email confirmation & (ii) matching two registration data points (e.g., DOB + phone). If unverifiable, we'll ask for more (photo ID). Response within a maximum period of 30 days; single 30-day extension possible. In Texas, we will respond to requests for access to PHI within 15 business days or less (Tex. Health & Safety Code § 181.103). Reasonable copy fees may apply. If we cannot verify your identity, we will inform you what additional information we need or deny the request. An authorized agent must submit a notarized letter or simple power of attorney along with proof of the requester's identity.

Revoking Authorizations

Revoke consents (e.g., marketing) any time via portal/email; revocation isn't retroactive.

14. Marketing & SMS (TCPA)

Opt-in gives express consent. Text "STOP" to cancel; "HELP" for help. Carrier rates may apply.

15. Reproductive-Health Data & Shield Laws

We do not disclose reproductive-health data to out-of-state authorities absent a valid federal order and will exhaust legal remedies.

16. Minors

Services for ages 18 years of age and older. No known collection from < 13.

17. Accessibility & Nondiscrimination (ACA §1557)

Policy in English/Spanish; free interpreters & accessible formats; no discrimination.

18. Third-Party Services & Sites

Review their policies before providing data.

19. Audio & Video Recordings

Not recorded by default. If consented, encrypted & deleted after 30 days. Whenever state law requires that telemedicine recordings be retained, Sana will store them in encrypted form for the minimum legally mandated period.

20. Contact Us

Privacy Officer: Sergio D. Capdevila

Email: privacidad@sanamujer.com

Phone: 1-248-574-2623 (Mon–Fri, 6 a.m.–1 p.m. Central Time CT)

Address: 5900 Balcones Dr STE 100, Austin, TX 78731

Last update: August 10, 2025