

Jaguar & Fern

Privacy Policy

Effective Date: June 11, 2026 **Privacy Officer:** Laurel Bougie, Founder — legal@jaguarandfern.com

Jaguar & Fern Marketing LLC, doing business as "Jaguar & Fern" ("Jaguar & Fern," "we," "our," or "us"), operates the Jaguar & Fern surgical scheduling platform (the "Platform") and our public marketing website at jaguarandfern.com (the "Website"). This Privacy Policy explains how we collect, use, share, secure, retain, and dispose of your information when you use the Platform to schedule an authorized surgical procedure, or when you visit our Website. This policy is one document covering both.

We provide this policy to you in plain language and ask you to affirmatively acknowledge that you have reviewed it before you authorize the Platform to access your health information.

1. Who We Are and What the Platform Does

The Platform helps you schedule a surgical procedure that your health plan has already approved. With your authorization, we use your health plan's Patient Access API to read your coverage and prior-authorization information, and we present in-network facilities and appointment times that match your approved procedure.

Jaguar & Fern operates as a Business Associate of the participating health systems whose care navigation teams coordinate your scheduling. We do not replace your care team's role in your care. All clinical decisions are made by you and your physician. We do not provide medical advice.

2. Information We Collect

A. Information from your health plan (with your express authorization)

With your OAuth 2.0 authorization, the Platform reads from your health plan's Patient Access API:

- Coverage and eligibility status
- Prior-authorization or pre-approval details and relevant dates
- Claims and Explanation of Benefits (EOB) records, including procedure codes and paid amounts used to calculate your routing options
- Demographic information (date of birth, address/ZIP code)

We read this information to present your scheduling options. We do not store your full name or insurance member ID in plain text.

B. Information you provide or select

- The facility and appointment slot you select
- Any optional preferences you enter during the scheduling flow

C. Operational records we create

When you complete a scheduling session, we create an operational record of that session. This record is used to operate the Platform, support quality review, and provide outcome reporting to the participating health system whose care team coordinated your scheduling. The record contains:

- A cryptographic hash of your insurance member ID and health system patient ID (a one-way transformation — your actual IDs are not stored)
- Your 5-digit ZIP code (used to calculate distance to facilities)
- Your procedure service line and relevant procedure (CPT) codes
- Prior-authorization status, approval dates, and expiry dates
- The facility and surgeon options you were presented with and the one you selected
- Financial indicators from your Explanation of Benefits used for reporting to the participating health system
- Session timing information (when you entered and made your selection)

Your name is not stored in these records. Your member ID and patient ID are stored only as cryptographic hashes.

D. Technical information

We collect limited technical information needed to operate and secure the Platform, including session and browser information, IP address, and security logs. We do not use third-party advertising trackers on the authenticated Platform.

3. How Your Information Is Used and Shared

- Presenting scheduling options: We use your health-plan information to identify in-network facilities and appointment times that match your approved procedure.
- Facility coordination: We share the information necessary to book your appointment with the care team of the facility you select.
- Reporting to the participating health system: We provide operational and outcome reports to the health system whose Navigator coordinated your scheduling. These reports are covered by our Business Associate Agreement with that health system. Reports are drawn from the operational records described in Section 2C and do not include your name or unmasked identifiers.
- Service providers: We share information with vendors who operate the Platform on our behalf, including Amazon Web Services (cloud hosting and database services). These vendors are bound by Business Associate Agreements or equivalent data-protection obligations and may use your information only to support our services.
- Legal compliance: We may disclose information if required by law, court order, or governmental authority, or to protect the rights, property, or safety of Jaguar & Fern, our users, or the public.

We do not sell your health information. We do not share it for advertising, marketing, or any purpose not described in this policy. We will not sell or share it for new purposes in the future without your express consent.

4. Express Consent

We obtain your express, informed consent before your health information is accessed, exchanged, or used, by (a) presenting this Privacy Policy for your affirmative acknowledgment before any data is accessed, and (b) directing you through your health plan's authorization screen (OAuth 2.0 with PKCE),

where you grant the Platform read access to your health-plan data. We will obtain separate, express consent before using or sharing your information for any purpose not described in this policy.

We do not use your information for marketing. The Platform does not make automated decisions that have legal or similarly significant effects on you or your care.

5. Information From Your Device

The Platform does not access any information from your device beyond the limited technical information described in Section 2D. We do not access your location, contacts, camera, microphone, photos, or any other device features.

6. How to Stop the Platform's Access

You can discontinue the Platform's access at any time by:

- Contacting us at legal@jaguarandfern.com, and
- Revoking the Platform's authorization through your health plan's member portal.

After you withdraw consent, we will stop accessing your health-plan data. Live session credentials (OAuth tokens, active session data) will be securely removed within 30 days. Operational records (Section 2C) are retained for 6 years as described in Section 9, except where a shorter period is legally sufficient.

7. Your Rights

Access: You may request a description of the information the Platform holds about you by contacting us at legal@jaguarandfern.com. We will respond within 30 days.

Correction: If you believe information we hold is inaccurate, contact us. Where the source data is held by your health plan or health system, we will direct you to your HIPAA right to request correction directly from them.

Deletion: Participating health systems may submit deletion requests on behalf of their members by contacting our Privacy Officer. Individual members may also contact us directly to request deletion of session data. Operational records may be retained for the period described in Section 9 to satisfy legal obligations.

Withdraw consent: You may withdraw your authorization at any time as described in Section 6. Withdrawal does not affect the lawfulness of any use that occurred before withdrawal.

8. How We Protect Your Information

We protect your information with administrative, technical, and physical safeguards, including:

- Encryption in transit and at rest for all health information stored or transmitted by the Platform
- Access controls limiting system access to authorized personnel only, with audit logging sufficient to satisfy our obligations under applicable law and our Business Associate Agreements
- Business Associate Agreements with all cloud infrastructure providers and service providers who handle health information on our behalf
- Dormant account handling: Accounts with no activity for 12 months will have their live access credentials revoked and session data removed. Operational records are retained per Section 9.

We comply with applicable breach notification laws. In the event of a breach affecting your health information, we will notify you and relevant authorities as required by law.

9. Data Retention

We retain operational records (Section 2C) for 6 years from the date of the scheduling session, consistent with the HIPAA-minimum retention standard, then securely destroy them. Live access credentials and session data are removed within 30 days of authorization revocation or account discontinuation.

10. Website Visitors

When you visit jaguarandfern.com, we collect limited technical information necessary to operate and secure the Website, including IP address, browser type, and pages visited. This information is used solely for website security and performance monitoring.

Contact Form: If you submit an inquiry through our contact form, your name, organization, role, email address, and message are collected and stored in HubSpot, our customer relationship management platform. We use this information solely to respond to your inquiry. We do not use it for marketing without your consent.

Cookies: Our website uses cookies necessary for basic website functionality and Google Analytics for anonymized usage reporting. We do not use advertising or targeting cookies. You can opt out of Google Analytics tracking at google.com/settings/ads.

We do not sell website visitor information.

11. Changes to This Policy; Business Transfers

We will proactively notify you of material changes to this policy and, where required, ask you to re-affirm your consent before continuing to use the Platform. In the event of a sale, merger, or wind-down of the business, we will, with respect to your health information, either (i) securely dispose of it; (ii) ensure the successor entity's commitments are at least as protective as this policy; or (iii) allow you to close your account and request deletion before any transfer occurs.

12. Children's Privacy

The Platform is intended for adult patients and is not directed to children under 13. We do not knowingly collect information from children. If you believe a child has provided information through the Platform, contact us at legal@jaguarandfern.com and we will promptly delete it.

13. No Targeted Advertising or Automated Decision-Making

We do not use your personal or health data for targeted advertising. The Platform presents scheduling options for you and your physician to consider; it does not make automated clinical decisions and does not produce automated decisions that have legal or similarly significant effects on you.

14. Accountability, Complaints, and Contact

Privacy Officer: Laurel Bougie, Founder

Privacy contact: legal@jaguarandfern.com

To exercise your rights, report a concern, or file a complaint:

- Contact us at legal@jaguarandfern.com with a description of your request or concern.
- We will acknowledge your message within 5 business days.
- We will investigate and provide a substantive response or remedy within 30 days.
- If you are not satisfied with our response, you may file a complaint with the Federal Trade Commission ([ftc.gov/complaint](https://www.ftc.gov/complaint)) or your state Attorney General's office.

We comply with applicable federal and state privacy laws and operate in accordance with the CARIN Alliance Code of Conduct.

15. About HIPAA and This Policy

When you direct the Platform to retrieve your health information from your health plan, you are exercising your individual right of access under HIPAA (45 CFR §164.524). Once your data is held by the Platform, this Privacy Policy and applicable federal law — including FTC Section 5(a) — and state law govern how we protect and use it. Jaguar & Fern operates as a Business Associate of participating health systems under executed Business Associate Agreements and handles all health information in accordance with those agreements.