

Wild Elm Privacy Policy

Version 1.0

Effective Date: July 9, 2026

Last Updated: July 9, 2026

Privacy Policy

1. Our Commitment to Privacy

At Wild Elm, we believe trust is foundational to healthcare. Patients trust providers with deeply personal information, providers trust their teams to coordinate care, and healthcare organizations trust technology to support critical operations.

We believe privacy should be understandable, transparent, and built into the architecture of the platform, not added later.

Wild Elm develops intelligent operational infrastructure for healthcare organizations. Our platform helps coordinate patient access, operational workflows, scheduling, communications, and organizational operations. Because our technology supports healthcare organizations, protecting information entrusted to us is one of our highest responsibilities.

This Privacy Policy explains how Wild Elm, Inc. ("Wild Elm," "we," "our," or "us") collects, uses, discloses, stores, and protects personal information when you:

- Visit our website;
- Request information or a demonstration of our platform;
- Use Wild Elm products or services;
- Interact with our communications;
- Apply for employment;
- Engage with us as a customer, vendor, or business partner.

This Privacy Policy also explains your privacy rights and the choices available to you under applicable privacy laws, including:

- United States privacy laws
- California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA)
- European Union General Data Protection Regulation (GDPR)
- United Kingdom GDPR
- Brazil's Lei Geral de Proteção de Dados (LGPD)

Privacy by Design

Privacy is not simply a compliance requirement, it is a design principle.

Wild Elm incorporates privacy and security considerations throughout the design, development, deployment, and operation of our platform. We strive to collect only the information necessary to deliver our services and apply appropriate administrative, technical, and organizational safeguards to protect that information.

When Wild Elm provides services to healthcare organizations, we process information only as necessary to deliver contracted services and in accordance with applicable laws, contractual obligations, and Business Associate Agreements where required.

2. Scope of this Privacy Policy

This Privacy Policy applies to information collected through:

- The Wild Elm website
- Product demonstrations
- Marketing communications
- Customer support interactions
- Customer portals
- Wild Elm software and cloud services
- Recruiting and employment activities
- Events and webinars
- Business development activities

This Privacy Policy does not apply to:

- Third-party websites linked from our website;
- Healthcare organizations that use Wild Elm;
- Information collected directly by healthcare providers;
- Third-party services integrated with Wild Elm that maintain their own privacy policies.

When Wild Elm provides software services to healthcare organizations, we generally process information on behalf of our customers. In those circumstances, the healthcare organization remains responsible for determining how personal information is collected and used within its organization.

If you are a patient of one of our customers and have questions regarding your medical information or patient records, please contact your healthcare provider directly.

3. Definitions

For purposes of this Privacy Policy:

"Personal Information"

Information that identifies, relates to, describes, or can reasonably be linked to an identified or identifiable individual.

Examples include:

- Name
- Email address
- Telephone number
- Mailing address
- IP address
- Device identifiers
- Online identifiers

The meaning of Personal Information may vary depending on applicable privacy law.

"Protected Health Information (PHI)"

"Protected Health Information" or "PHI" has the meaning assigned under the Health Insurance Portability and Accountability Act ("HIPAA") and generally refers to individually identifiable health information maintained or transmitted by a covered entity or business associate.

"Customer"

Any healthcare organization, provider, clinic, health system, medical group, or other organization that licenses or uses Wild Elm services.

"Patient"

An individual receiving healthcare services from one of our Customers.

Wild Elm generally processes patient information solely on behalf of healthcare organizations.

"Processing"

Any operation performed on information including collecting, storing, organizing, using, transmitting, analyzing, modifying, or deleting information.

"Services"

The Wild Elm platform, website, applications, APIs, communications, workflows, software, and related services.

4. Information We Collect

The information we collect depends on how you interact with Wild Elm.

In some situations, we collect information directly from you.

In other situations, we receive information from our Customers or automatically through our technology.

a. Information You Provide Directly

You may voluntarily provide information when you:

- Request a product demonstration
- Contact us
- Complete a web form
- Subscribe to communications
- Register for webinars or events
- Apply for employment
- Request customer support
- Communicate with Wild Elm personnel

Depending on the interaction, this information may include:

- Name
- Company name
- Job title
- Email address
- Telephone number
- Business address
- Professional information
- Communication preferences
- Information contained in messages you send us

We collect only information reasonably necessary to respond to your request or provide requested services.

b. Information Collected Automatically

When you visit our website or use our Services, we may automatically collect certain technical information.

Examples include:

- IP address
- Browser type
- Operating system
- Device identifiers
- Language preferences
- Time zone
- Referring website
- Pages viewed
- Time spent on pages
- Navigation patterns
- Date and time of access
- Error logs
- Diagnostic information

This information helps us:

- Improve website performance
- Monitor security
- Detect fraud
- Troubleshoot issues
- Understand website usage
- Improve user experience

This information generally does not directly identify you by itself, although it may be considered Personal Information under certain privacy laws.

c. Information Provided by Customers

Healthcare organizations using Wild Elm may provide information necessary for the operation of our Services.

Depending upon the customer's implementation, this may include:

- Operational Information
- Appointment information
- Scheduling data
- Resource availability
- Provider schedules
- Operational workflows
- Referral information

- Communications metadata
- Waitlist information
- Capacity information
- Patient Contact Information

When authorized by our Customers, Wild Elm may process information such as:

- Patient name
- Telephone number
- Email address
- Preferred communication method
- Appointment history
- Communication history

Where applicable, this information may constitute Protected Health Information under HIPAA.

Wild Elm processes this information only as instructed by our Customers and consistent with applicable Business Associate Agreements.

d. Information from Third Parties

We may receive information from trusted third-party sources including:

- CRM systems
- Marketing platforms
- Authentication providers
- Identity verification services
- Communication providers
- Integration partners
- Analytics providers
- Recruiting platforms

We use this information only for legitimate business purposes consistent with this Privacy Policy.

e. Information We Do Not Intentionally Collect

Wild Elm does not intentionally collect information unrelated to providing our Services.

We do not intentionally collect:

- Personal information from children under applicable legal ages;
- Sensitive information unrelated to healthcare operations;
- Personal information for unrelated advertising purposes.

We do not sell Personal Information.

5. How We Use Information

Wild Elm uses information only for legitimate business purposes consistent with applicable law and our contractual obligations.

Depending on your interaction with us, we may use information to:

a. Deliver Our Services

Including:

- Operating the Wild Elm platform
- Coordinating operational workflows
- Scheduling appointments
- Managing communications
- Supporting patient access
- Authenticating users
- Delivering requested functionality

b. Support Our Customers

Including:

- Responding to support requests
- Troubleshooting issues
- Monitoring service availability
- Providing implementation assistance
- Delivering product updates
- Improving customer experience

c. Improve Our Products

We continuously evaluate how our platform performs in order to:

- Improve usability
- Enhance reliability
- Develop new features
- Improve workflow coordination
- Improve operational intelligence
- Optimize system performance
- Conduct research and product development

Where feasible and appropriate, we use aggregated or de-identified information for product improvement activities.

d. Communicate With You

Including:

- Responding to inquiries
- Scheduling demonstrations
- Sending requested information
- Product announcements
- Service notifications
- Security notifications
- Customer communications

- Marketing communications (where permitted by law)

You may opt out of marketing communications at any time. Transactional or service-related communications may continue where necessary to provide our Services.

e. Protect Our Services

We use information to help:

- Detect fraud
- Prevent unauthorized access
- Monitor cybersecurity threats
- Investigate suspicious activity
- Maintain system integrity
- Protect our Customers
- Enforce our agreements

Protecting healthcare information requires continuous monitoring and responsible security practices.

f. Comply with Legal Obligations

We may process information to:

- Comply with applicable laws
- Respond to lawful requests
- Meet contractual obligations
- Protect legal rights
- Resolve disputes
- Support audits and regulatory requirements

g. Business Operations

We also use information for normal business operations, including:

- Financial reporting
- Corporate governance
- Vendor management
- Risk management
- Insurance
- Business continuity planning
- Strategic planning
- Internal administration

Guiding Principles

Regardless of the specific purpose, Wild Elm seeks to process information according to four guiding principles:

- **Purpose Limitation** – We collect and use information only for legitimate, disclosed purposes.
- **Data Minimization** – We collect only the information reasonably necessary to provide our Services.

- **Security by Design** – Privacy and security considerations are incorporated throughout our platform and operational practices.
- **Customer Control** – Healthcare organizations retain ownership and control of their data. Wild Elm processes customer information only as necessary to provide contracted services.

6. Artificial Intelligence & Automated Processing

Wild Elm uses artificial intelligence ("AI"), machine learning, deterministic rules, and optimization algorithms to support operational workflows within healthcare organizations.

Our platform is designed to improve operational coordination, not replace clinical judgment.

Depending on the services a Customer has implemented, Wild Elm may use AI to assist with activities such as:

- Appointment scheduling and rescheduling
- Patient communication
- Intelligent message routing
- Operational workflow coordination
- Waitlist management
- Capacity forecasting
- Operational recommendations
- Administrative automation
- Workflow prioritization
- Demand forecasting
- Resource optimization

AI capabilities are always deployed within defined operational guardrails established by Wild Elm and our Customers.

Human Oversight

Wild Elm believes AI should augment human decision-making, not eliminate it.

Our platform is designed to support healthcare organizations by reducing administrative burden while preserving appropriate human oversight.

Depending on workflow configuration, automated recommendations may:

- Require staff approval;
- Escalate to designated personnel;
- Trigger review based on confidence thresholds;
- Follow customer-defined business rules; or
- Execute automatically only where appropriate and authorized.

Healthcare organizations remain responsible for determining which operational workflows should include human review.

Clinical Decision Making

Wild Elm is not intended to diagnose, treat, prescribe, or make independent clinical decisions. The platform supports operational coordination surrounding healthcare delivery.

Wild Elm does not replace the professional judgment of physicians, nurses, or other licensed healthcare professionals.

Clinical decisions remain solely the responsibility of qualified healthcare providers.

Continuous Improvement

We may use aggregated, de-identified, or anonymized operational information to improve the quality, safety, reliability, and performance of our Services.

Where required by law or contract, Wild Elm does not use identifiable customer information or Protected Health Information to train generalized AI models without appropriate authorization.

AI Transparency

Wild Elm believes intelligent systems should remain transparent.

Where practical, our platform is designed to support:

- Explainable operational recommendations
- Configurable business rules
- Auditability
- Human oversight
- Operational accountability

We believe organizations should understand how operational decisions are made, not simply trust that they were.

7. Protected Health Information (HIPAA)

When Wild Elm provides services to healthcare organizations that are subject to the Health Insurance Portability and Accountability Act ("HIPAA"), we may receive, maintain, or process Protected Health Information ("PHI") as a Business Associate.

In those circumstances:

- The healthcare organization remains the Covered Entity (or Business Associate, as applicable);
- Wild Elm acts only as authorized under the applicable agreement;
- Processing is governed by applicable Business Associate Agreements ("BAAs");
- Wild Elm processes PHI solely to provide contracted services.

Wild Elm does not use PHI for unrelated commercial purposes.

Minimum Necessary Principle

Wild Elm follows the HIPAA principle of minimum necessary use and disclosure.

Where applicable, access to PHI is limited to personnel and systems that require such access to perform authorized responsibilities.

Access controls are designed to minimize unnecessary exposure while supporting operational workflows.

Safeguards

Wild Elm maintains administrative, technical, and organizational safeguards designed to protect PHI, including measures intended to support:

- Confidentiality
- Integrity
- Availability
- Access control
- Auditability
- Workforce accountability

Additional information regarding our security practices is available through our **Trust Center**.

8. Customer Data Ownership

Healthcare organizations retain ownership of their data.

Wild Elm does not acquire ownership rights to customer information, patient records, operational workflows, or Protected Health Information through the use of our Services.

Except as required to provide contracted services, comply with applicable law, or fulfill contractual obligations, Wild Elm does not use customer information for independent business purposes.

Customer Control

Customers determine:

- What information is entered into the platform;
- Which workflows are enabled;
- User access permissions;
- Data retention settings (where configurable);
- Authorized integrations;
- Communication preferences.

Wild Elm processes customer information only in accordance with applicable agreements and documented customer instructions.

Data Portability

Upon termination of services, Customers may request export of their data in accordance with applicable agreements.

Data deletion and retention practices are described later in this Privacy Policy.

9. Business Associate Agreements

When required by HIPAA, Wild Elm enters into Business Associate Agreements with Covered Entities and other Business Associates.

Our BAAs define:

- Permitted uses of PHI;
- Required safeguards;
- Reporting obligations;
- Subcontractor responsibilities;
- Breach notification requirements;
- Return or destruction of PHI where applicable.

Business Associate Agreements supplement, not replace this Privacy Policy.

10. How We Share Information

Wild Elm does not sell Personal Information.

We disclose information only where necessary to operate our Services, fulfill contractual obligations, comply with legal requirements, or protect legitimate business interests.

Service Providers

We may share information with trusted vendors that assist us in providing our Services.

Examples include providers of:

- Cloud infrastructure
- Hosting
- Communications
- Authentication
- Customer support
- Analytics
- Security monitoring
- Identity verification
- Payment processing
- Recruiting
- Productivity software

These providers are contractually required to protect information consistent with applicable law and our contractual obligations.

Customer Instructions

Where Wild Elm acts on behalf of healthcare organizations, information may be disclosed only as instructed by the applicable Customer.

Examples include:

- Appointment reminders;
- Patient communications;
- Referral coordination;
- Scheduling workflows;
- Authorized integrations.

Legal Requirements

We may disclose information where required to:

- Comply with applicable law;
- Respond to lawful governmental requests;
- Protect legal rights;
- Prevent fraud;
- Enforce agreements;
- Protect the safety of individuals.

Where legally permitted, we may notify Customers before responding to requests involving customer information.

Corporate Transactions

If Wild Elm is involved in a merger, acquisition, financing, reorganization, asset sale, or similar transaction, information may be transferred as part of that transaction subject to applicable confidentiality obligations.

11. Cookies & Similar Technologies

Wild Elm uses cookies and similar technologies to improve website functionality, security, analytics, and user experience.

Cookies are small data files stored on your device that help websites recognize your browser and remember certain information.

a. Types of Cookies

i. Essential Cookies

1. Necessary for:
 - a. Website operation;
 - b. Authentication;
 - c. Security;
 - d. Session management.
2. These cookies cannot generally be disabled without affecting website functionality.

ii. Functional Cookies

1. Used to remember:
 - a. Language preferences;
 - b. User settings;
 - c. Accessibility preferences.
 - d. Analytics Cookies
2. Help us understand:
 - a. Website traffic;
 - b. Visitor behavior;
 - c. Feature usage;
 - d. Performance;
 - e. Navigation patterns.
3. Analytics information is generally aggregated whenever practical.

iii. Marketing Cookies

1. If Wild Elm engages in marketing campaigns, cookies may be used to understand campaign effectiveness and improve communications.
2. Where required by law, we will request consent before placing non-essential cookies.

b. Cookie Choices

- i. Depending upon your location, you may:
 1. Accept or reject non-essential cookies;
 2. Modify browser settings;
 3. Delete previously stored cookies;
 4. Withdraw consent.

Additional information is available in our Cookie Policy.

12. Data Security

Protecting customer information is one of Wild Elm's highest priorities.

We maintain administrative, technical, and organizational safeguards designed to protect information against unauthorized access, disclosure, alteration, or destruction.

No system can guarantee absolute security. However, Wild Elm continually evaluates and improves its security practices to address evolving threats.

Security Measures

Our security program includes measures such as:

- Encryption in transit
- Encryption at rest
- Least-privilege access controls
- Multi-factor authentication
- Identity and access management
- Secure software development practices
- Vulnerability management
- Infrastructure monitoring
- Audit logging
- Incident response procedures
- Vendor risk management
- Workforce security training

Security controls evolve continuously as our platform and threat landscape change.

Security Monitoring

Wild Elm continuously monitors our infrastructure and services for indicators of unauthorized access, misuse, or security threats.

Monitoring activities help support:

- System availability;
- Threat detection;

- Incident investigation;
- Performance optimization;
- Operational resilience.

Security Incidents

Wild Elm maintains documented procedures for responding to security incidents.

Where required by applicable law or contractual obligations, affected Customers will be notified of qualifying security incidents in accordance with applicable agreements and legal requirements.

Trust Center

Wild Elm maintains a public **Trust Center** providing additional information regarding our security posture, governance practices, compliance initiatives, and related documentation.

For the latest information regarding our security program, please visit our Trust Center:

Trust Center

Security Philosophy

Security is not simply a compliance exercise.
It is a continuous operational discipline.

Wild Elm incorporates security, privacy, governance, and accountability into the design and operation of our platform because healthcare organizations deserve technology they can trust.

13. Data Retention

Wild Elm retains Personal Information only for as long as necessary to fulfill the purposes described in this Privacy Policy, satisfy our contractual obligations, comply with applicable law, resolve disputes, enforce our agreements, and protect the security and integrity of our Services.

Retention periods vary depending on the type of information and the purpose for which it was collected.

Examples include:

Information Type	Typical Retention Basis
Website inquiries	Until request is resolved or no longer needed for business records
Marketing preferences	Until consent is withdrawn or communications cease
Customer account information	Duration of the customer relationship plus applicable legal retention periods
Operational logs	Based on security, audit, contractual, and regulatory requirements
Customer data	As directed by the applicable customer agreement
Employment applications	As required by applicable employment laws

Where practical and legally permissible, information may be anonymized or aggregated for statistical, security, product improvement, or operational analysis purposes.

Upon termination of a customer's subscription, Wild Elm will return or delete customer data in accordance with applicable agreements, Business Associate Agreements, and legal obligations.

14. Your Privacy Rights

Privacy rights vary depending on your jurisdiction.

Wild Elm is committed to honoring applicable privacy rights under relevant laws.

United States

Individuals located in the United States may have rights under applicable federal and state privacy laws.

Depending on your jurisdiction, these rights may include:

- Access to personal information;
- Correction of inaccurate information;
- Deletion of personal information;
- Portability of certain information;
- Withdrawal of marketing communications;
- Information regarding categories of collected information.

Wild Elm will respond to applicable requests in accordance with governing law.

California Privacy Rights (CCPA / CPRA)

If you are a California resident, you may have additional rights under the California Consumer Privacy Act ("CCPA"), as amended by the California Privacy Rights Act ("CPRA").

These rights may include:

- The right to know the categories of Personal Information collected;
- The right to know the sources of Personal Information;
- The right to know how Personal Information is used;
- The right to know categories of third parties receiving Personal Information;
- The right to request deletion of Personal Information;
- The right to request correction of inaccurate information;
- The right to request access to Personal Information;
- The right to data portability;
- The right to limit certain uses of Sensitive Personal Information where applicable;
- The right not to be discriminated against for exercising privacy rights.

Sale and Sharing of Personal Information

Wild Elm does not sell Personal Information.

Wild Elm does not sell Protected Health Information.

Wild Elm does not knowingly share Personal Information for cross-context behavioral advertising as defined by applicable California law.

California residents may submit privacy requests using the contact information provided at the end of this Privacy Policy.

European Economic Area (GDPR)

If you are located in the European Economic Area ("EEA"), Wild Elm processes Personal Data in accordance with the General Data Protection Regulation ("GDPR").

Legal Bases for Processing

Depending on the circumstances, Wild Elm may process Personal Data based upon:

- Performance of a contract;
- Compliance with legal obligations;
- Legitimate business interests;
- Consent (where required);
- Protection of vital interests;
- Public interest where applicable.

GDPR Rights

Subject to applicable law, individuals may have the right to:

- Access Personal Data;
- Correct inaccurate Personal Data;
- Request deletion ("Right to be Forgotten");
- Restrict processing;
- Object to certain processing activities;
- Receive Personal Data in a portable format;
- Withdraw consent where processing is based upon consent;
- Lodge a complaint with an appropriate supervisory authority.

Wild Elm will respond to verified requests within applicable legal timeframes.

United Kingdom (UK GDPR)

Individuals located in the United Kingdom have similar rights under the UK General Data Protection Regulation and the UK Data Protection Act.

Wild Elm processes Personal Data in accordance with applicable UK privacy legislation and honors applicable rights relating to:

- Access
- Rectification
- Erasure
- Restriction
- Portability
- Objection
- Withdrawal of consent

Complaints may also be submitted to the UK Information Commissioner's Office (ICO).

Brazil (LGPD)

For individuals located in Brazil, Wild Elm processes Personal Data in accordance with Brazil's Lei Geral de Proteção de Dados ("LGPD").

Subject to applicable law, Brazilian data subjects may have rights including:

- Confirmation of processing;
- Access to Personal Data;
- Correction of incomplete or inaccurate information;
- Anonymization or deletion where appropriate;
- Data portability;
- Information regarding data sharing;
- Revocation of consent;
- Information regarding automated decision-making where applicable.

Complaints may also be submitted to Brazil's National Data Protection Authority (ANPD).

15. Exercising Your Privacy Rights

To exercise applicable privacy rights, please contact Wild Elm using the information provided at the end of this Privacy Policy.

To protect the privacy and security of individuals, we may request information necessary to verify identity before responding to a request.

Certain requests may be denied where permitted by applicable law, including where fulfilling the request would:

- Violate legal obligations;
- Affect the rights of others;
- Interfere with regulatory requirements;
- Prevent Wild Elm from fulfilling contractual obligations;
- Conflict with HIPAA or other healthcare regulations.

If we deny a request, we will explain the reason where required by law.

16. International Data Transfers

Wild Elm operates internationally and may process information in countries other than the country in which it was originally collected.

Where Personal Data is transferred internationally, Wild Elm implements appropriate safeguards designed to protect information consistent with applicable privacy laws.

Depending upon the jurisdiction, these safeguards may include:

- Standard Contractual Clauses (SCCs);
- Adequacy decisions;
- Contractual protections;
- Technical and organizational safeguards;
- Other legally recognized transfer mechanisms.

17. Children's Privacy

Wild Elm's website and Services are not directed toward children.

We do not knowingly collect Personal Information directly from children under the age required by applicable law without appropriate authorization.

If we become aware that Personal Information has been collected from a child in violation of applicable law, we will take appropriate steps to delete such information.

Parents or guardians who believe information may have been collected from a child may contact us using the information provided below.

18. Third-Party Websites & Services

Our website may contain links to third-party websites, applications, integrations, or services.

This Privacy Policy does not apply to information collected by third parties.

Wild Elm encourages users to review the privacy practices of any third-party services they access.

Wild Elm is not responsible for the privacy practices or content of third-party websites.

19. Changes to this Privacy Policy

Wild Elm may update this Privacy Policy periodically to reflect:

- Changes in applicable law;
- New products or services;
- Changes in technology;
- Security improvements;
- Operational changes;
- Regulatory guidance.

When material changes are made, we will update the "Last Updated" date at the beginning of this Privacy Policy.

Where required by law, we will provide additional notice or obtain consent before material changes become effective.

20. Contact Us

Questions regarding this Privacy Policy or Wild Elm's privacy practices may be directed to:

Wild Elm, Inc.

188 Front Street
Suite 116-58
Franklin, TN 37064
Attn: Privacy Officer

Email: privacy@wildelm.io

Website: www.wildelm.io

Individuals submitting privacy requests should include sufficient information to allow us to verify their identity and respond appropriately.

21. Governing Law

This Privacy Policy shall be governed by and interpreted in accordance with the laws specified in Wild Elm's Terms of Service, except where superseded by mandatory privacy laws applicable to the individual exercising privacy rights.

Nothing in this Privacy Policy limits any rights available under applicable privacy legislation.

Related Resources

For additional information regarding Wild Elm's security and governance practices, please visit:

- [Terms of Service](#)
- [Cookie Policy](#)
- [Trust Center](#)
- [Security Overview](#)
- [Responsible AI Statement](#)
- [Accessibility Statement](#)
- [Subprocessor List](#)

At Wild Elm, we believe trust is earned through transparency, accountability, and thoughtful engineering, not simply through compliance.

Our privacy program is guided by six principles:

- **Privacy by Design** - Privacy considerations are incorporated throughout the lifecycle of our platform.
- **Customer Ownership** - Healthcare organizations retain ownership and control of their data.
- **Security by Default** - We design our platform to support strong security and operational resilience.
- **Transparency** - We strive to explain how information is collected, used, and protected in clear language.
- **Responsible AI** - Artificial intelligence supports operational workflows while remaining subject to appropriate oversight and safeguards.
- **Continuous Improvement** - We continually evolve our privacy and security practices to meet changing technology, threats, and regulatory expectations.