

Privacy Policy

Effective date: October 1, 2026

One Wolf Inc. operates Credentialing Agents ("we," "us," or "our"). This policy explains how we collect, use, disclose, retain, and protect personal information through our website, client-operated platform, clinician and candidate portals, integrations, and communications. It covers website visitors, business contacts, client users, clinicians, applicants, references, and others involved in our services in the United States, Canada, and the United Kingdom.

Our role and the client's role

For our website, business inquiries, account administration, billing, marketing preferences, and our own security and legal obligations, One Wolf determines the purposes and means of processing and acts as a controller or business where those terms apply. Where we provide a service directly at a clinician's request and determine its purposes and means, we are responsible for that processing in our own capacity.

Most credentialing information is processed on instructions from a staffing company, healthcare organization, or other client. We ordinarily act as its processor or service provider, administering document collection, communications, record retrieval, and workflow tracking. The client determines its credentialing requirements, authorized uses and recipients, retention requirements, and final decisions. Using agents to perform these tasks does not transfer the client's institutional credentialing or decision-making responsibilities to us.

The client's privacy notice explains its uses of your information. Applicable client agreements, data processing addenda, and business associate agreements govern our processing on its behalf. This policy does not expand those permissions or remove rights required by law. Contractual ownership of a file does not remove an individual's privacy rights, and an individual's access rights do not necessarily extend to every item in a client's file.

Information we process and its sources

Contact and account information. Names, work and personal contact details, organization, role, user identifiers, access permissions, authentication records, and communication preferences. Sources include you, client administrators, and connected account services.

Website, demo, and subscription information. When you request a demo, join a waitlist, subscribe to our blog, or contact us through the website, we collect your name, work email, and phone number, and any company, role, or message you choose to share. If you request a recorded demo, we may send a one-time verification code to your email address or phone. Website forms use a security check to block automated abuse.

Professional and credentialing information. Licenses, professional identifiers, education, certifications, qualifications, employment and placement history, references, attestations, signatures, eligibility information, disciplinary records, and documents or results supplied by clients, individuals, sources, and authorized vendors.

Sensitive information. Depending on the client's credentialing requirements and the documents involved, we handle Social Security and other government identification numbers, government IDs, dates of birth, work authorization information, financial details, vaccination and other health records, medical examinations, drug-test results, background-check reports, and criminal history information. Files may also contain patient information, photographs, biometric information such as fingerprints, facial scans or voiceprints, precise location, or other sensitive details supplied or obtained for an authorized credentialing purpose. The categories used vary by workflow; we do not require every category from every person. We describe applicable purposes and any additional permissions at the relevant collection or workflow stage.

Communications and workflow information. Emails and attachments, text messages, call details and transcripts, support requests, approvals, extracted fields, summaries, discrepancy flags, status updates, and audit records. We transcribe calls for the relevant workflow but do not retain call audio. Live audio is processed as needed to conduct and transcribe the call.

Business and transaction information. Subscription selections, usage quantities, invoices, payment status, billing contacts, and financial details necessary for the relevant transaction or authorized workflow.

Technical and website information. IP address, approximate location inferred from IP address, device and browser information, pages visited, referral sources, timestamps, interactions, cookies, and similar identifiers. We obtain this information from devices and service providers, subject to applicable choices.

Information comes from you; clients and their authorized users; connected ATS, CRM, email, and other systems; references, facilities, educational institutions, licensing boards, public registries and websites; and client-authorized vendors. Within an enabled credentialing workflow, agents may independently search for additional relevant information and retrieve it from these sources, without a separate instruction for each search. Public availability does not authorize unrelated reuse.

Connected systems may give agents permission to read mailbox messages and attachments and to take enabled actions. Depending on the permissions granted, access may extend beyond an individual credentialing message or folder. We use that access for the authorized service and generally retain retrieved content only when needed to perform or document the work. Connection settings and permission scopes determine actual access. Disconnecting a system stops future access through that connection; information already incorporated into a workspace follows its retention rules.

Do not send clinician records, patient information, or sensitive identifiers through public demo or marketing forms. Use the client's authorized submission channels.

How we use information

We use information to administer client-enabled credentialing and onboarding workflows, collect and organize documents, retrieve records, coordinate requests and vendor services, communicate with participants, track requirements and expirations, maintain audit records, and export information to authorized systems. Clients may use the platform as their primary credentialing record or alongside an ATS or CRM. We provide standard onboarding and technical support and any separately elected human administrative supervision.

We use business and technical information to operate accounts, administer billing and usage, protect systems, prevent misuse, investigate incidents, resolve disputes, meet legal obligations, and improve service reliability. Client records are used for these purposes only within the client's authorization and applicable restrictions.

We use website and business contact information to respond to inquiries, arrange demonstrations, and send permitted business communications. Website analytics and advertising are described below. We do not use client credentialing information for our advertising, a shared recruiting directory, or unrelated products. Sharing for another organization's workflow requires an appropriate client or clinician instruction or authorization.

Clinicians may ask us to help them access, retrieve, download, or share their documents and information with a recipient they identify. We may carry out those requests after verifying identity, authority, and the permitted scope. Client-controlled records, third-party restrictions, other people's information, and applicable law may require additional authorization or limit what can be released. A request does not grant general access to another client's workspace or automatically extend the originating workspace's retention period.

Information required for a particular workflow depends on its purpose. Declining to provide necessary information, withdrawing a permission, or disabling an integration may prevent completion of that workflow. The client decides any resulting employment or credentialing consequences.

AI agents and human review

AI agents process documents, messages, and authorized records to extract and classify information, prepare summaries, compare information against client-approved requirements, identify discrepancies, and take enabled routine actions automatically. Actions can include searching public sources, requesting documents, sending email or texts, conducting AI-

assisted calls, and updating connected systems. Outputs and flags may affect follow-up requests and routing for human review.

We primarily use self-hosted AI models and also use external AI providers for selected tasks. Relevant documents, message content, instructions, or extracted information may be sent to those providers to perform the task. We do not use personal information processed through our services to train or fine-tune AI models, and we do not permit our AI providers to do so. Using existing records to answer a request or correct a workflow is distinct from model training. Provider processing and any technical retention remain subject to applicable service restrictions; the no-training restriction does not itself mean zero retention. Clients may request current provider and processing details.

Agents can make mistakes, including incorrect extraction, summaries, or conclusions. We recommend human supervision. Clients may designate their own reviewers or elect our administrative supervision service. We do not independently make final hiring, assignment, clinical privileging, or institutional credentialing decisions. If you believe information or an automated output is incorrect, contact the organization managing your file or our privacy contact to request correction or human review. The client remains responsible for decisions it makes using the platform.

We do not sell client credentialing records, use them for advertising, or reuse them for unrelated purposes. Authorized employees, contractors, or elected supervisors may review records to provide the service, investigate an issue, or respond to a valid request. Access is limited to the work they are authorized to perform.

Communications and your choices

On a client's instructions, agents may communicate with clinicians, staff, references, facilities, and vendors by email, SMS/text, and telephone, including automated messages and AI-generated voice. We provide applicable notices, consent mechanisms, and opt-out options. Where notice or consent is required for AI voice or transcription, it must be provided or obtained for that interaction. We retain the resulting transcript for the authorized workflow, not the call audio.

Text messages. We send text messages through our messaging provider, Twilio. Messages include one-time verification codes you request on our website and, on a client's instructions, credentialing workflow messages such as document requests, reminders, and status updates. Where consent is required, we send text messages only after it has been given. Message frequency varies by workflow. Message and data rates may apply. Reply STOP to stop text messages at any time; we send one message confirming the opt-out. Reply HELP for help, or email privacy@credentialingagents.com. Carriers are not liable for delayed or undelivered messages.

Mobile information. We do not share mobile information with third parties or affiliates for marketing or promotional purposes. Text messaging originator opt-in data and consent are excluded from every category of recipient described in this policy and are not shared with any third party, except service providers that deliver messages for us, such as Twilio, or where the law requires.

You can reply STOP to an SMS or use another stated opt-out method. You may also tell the caller, client, or our privacy contact that you wish to stop a communication channel. We honor valid revocations and suppression requirements. A client's instruction to contact you is not a substitute for legally required consent. You can request an alternative way to complete the process from the client.

Email. We send email through our email provider, SparkPost. Blog subscriptions use double opt-in: you are added only after you confirm from the email we send. Every marketing email includes an unsubscribe link and our postal address, and we process unsubscribe requests within 10 business days. Marketing emails record opens and clicks so we can measure engagement. Essential account, security, and requested service communications may continue through permitted channels. Where Canada's Anti-Spam Legislation applies, we send commercial electronic messages only with the required consent, identification, and unsubscribe mechanism.

Who receives information

Clients and their authorized recipients. Client administrators and designated reviewers, and facilities, verification sources, references, or vendors selected or approved for the workflow. We share only information needed for the authorized purpose; a reference request does not authorize disclosure of an entire credentialing file.

Service providers and personnel. Amazon Web Services (AWS) provides our principal hosting infrastructure. Our public website is hosted by Vercel, and it uses SparkPost for email, Twilio for text messages, Cloudflare Turnstile for form security, Cal.com for demo scheduling, and Vimeo for recorded demo video. External AI providers and any other authorized providers supporting an enabled service may process relevant information for us. Authorized employees, contractors, and elected human supervisors may access information for their assigned work. Providers processing client information on our behalf are subject to applicable confidentiality, security, and purpose restrictions. Clients can request current subprocessor and processing-location details through our privacy contact; applicable contractual notice and authorization procedures govern changes.

Recipients you request. We may share documents with a recipient identified by a clinician, subject to the checks and restrictions described above. A recipient that determines its own uses of information is responsible for those uses under its own privacy notice.

Independent services. A client's ATS, CRM, screening vendor, or other selected external service may process information under its own agreement and privacy notice. We send information to these services within the relevant authorization. Their practices may differ from ours. Advertising platforms receiving website information are addressed below.

Legal and business circumstances. Where legally required, or as permitted to protect rights, investigate misuse, or respond to legal claims, we may disclose necessary information to authorities, advisers, or other appropriate recipients. In a merger, financing, reorganization, or sale of a business, information may be disclosed subject to appropriate confidentiality and continued privacy protections. These circumstances do not authorize unrestricted reuse of client records.

Website cookies and advertising

Our public marketing website groups cookies and similar technologies into three purposes. These marketing analytics and advertising trackers are not used in the product application or clinician portal. Operational product logs and security records are handled separately.

Strictly necessary. Technologies required to operate and secure the site, protect forms from abuse, keep a session you start (such as a recorded-demo viewing session), and remember your cookie choice for 180 days. These are always active.

Analytics. Google Analytics 4 helps us understand traffic and improve the site.

Advertising and retargeting. Meta Pixel (Facebook and Instagram), LinkedIn Insight Tag, TikTok Pixel, and Google Ads tools measure campaigns and show relevant ads to people who have visited the site.

Analytics and advertising tools load through Google Tag Manager only after you accept them. Until then, Google Consent Mode keeps analytics and advertising storage denied. When you schedule a demo or watch a recorded demo, Cal.com or Vimeo may set their own cookies under their own privacy notices.

Website advertising tools can disclose device identifiers, IP addresses, browsing activity, and related online interactions to advertising platforms. Those platforms may act as independent controllers. We do not sell personal information for money; advertising disclosures can nevertheless constitute a sale, sharing, or targeted advertising under some privacy laws. This website advertising activity is separate from client credentialing records, which we do not provide for advertising or retargeting.

Use the Cookie settings link in the website footer to reject or withdraw optional analytics and advertising choices. Rejection blocks the relevant optional trackers. If your browser sends a Global Privacy Control signal, we treat it as a rejection and do not load optional analytics or advertising tools; we also honor other applicable legally required opt-out signals. These

controls also allow you to opt out of website disclosures that qualify as sale, sharing, or targeted advertising. You can contact us if the controls are inaccessible.

Browser controls can restrict cookies, although some functions may be affected. Preferences may need to be set separately on each browser or device. Third-party advertising platforms maintain their own privacy notices and controls.

How we protect information

We use administrative, technical, and physical safeguards designed to protect personal information. These include encryption in transit and at rest, restrictions on authorized access, separation of client workspaces, access logs, backups, and incident response procedures. Access to client information is limited by role and service need. We remain responsible for safeguards within our control; clients are responsible for their user permissions, devices, and connected accounts. No system or transmission method can be guaranteed completely secure. We investigate security incidents and provide notices as required by applicable law and agreements.

Workspace retention and deletion

Retention is tied to the client workspace, not an individual placement. While a workspace remains active, we maintain credentialing files and related workflow records, including relevant transcripts and audit records, in accordance with the client's instructions and applicable requirements. A placement ending does not itself trigger deletion. This supports the client's ongoing credentialing, recordkeeping, and audit needs.

Our standard policy is to retain workspace information for 90 days after the workspace is terminated, then delete its active records. Clients should arrange any required export before that period ends. A different documented arrangement or a specific legal preservation requirement may affect deletion. Valid requests or legal obligations may also require correction, restriction, or earlier deletion; an active workspace does not override those requirements.

Residual backup copies may remain temporarily after active-system deletion until removed through the applicable backup rotation and deletion process. Such copies remain protected and restricted from ordinary use. Information retained for a legal obligation is limited to that purpose and deleted when no longer required. Clients may request the backup deletion schedule applicable to their workspace.

For information we handle in our own capacity, retention depends on the purpose, the ongoing relationship or request, accounting and legal requirements, dispute periods, and security needs. This includes business contacts, demo requests, billing, privacy requests, and any separately requested clinician document service. We retain only what remains necessary

for those purposes. Minimal suppression records may be kept to honor opt-outs. Website cookie and analytics retention depends on the relevant purpose and tool configuration; details can be requested through our privacy contact.

Sensitive information

Sensitive information is handled for the authorized credentialing or document-management purpose, subject to applicable permissions and safeguards. Client instructions do not replace any legally required notice, consent, lawful basis, or restriction. Biometric, health, and criminal history information may require additional notices, authorizations, retention rules, or agreements for the particular workflow. This policy does not itself provide consent for biometric identification or authorize unrestricted collection of sensitive information.

Where information is protected health information and we act as a business associate, applicable HIPAA requirements and a separate business associate agreement govern that processing. Health-related employment records are not automatically subject to HIPAA. This policy is not a HIPAA Notice of Privacy Practices. Patient information should be supplied only where necessary for an authorized workflow and covered by the required arrangements.

Hosting and international processing

Our platform's primary AWS hosting region is US East (Northern Virginia), us-east-1. Our public website is served through Vercel's network. We maintain distributed backups. Primary hosting does not mean every backup, AI-processing operation, or service component is confined to that region. Information may be processed in the United States and in other countries where authorized providers operate. Personnel currently authorized to access client records are based in the United States. We may authorize personnel in other countries in the future, subject to access restrictions, client commitments, and applicable law.

If you are in Canada or the UK, using our service involves processing information outside your country. Privacy laws may differ, and information may be accessible to courts, law enforcement, or other authorities under the laws of the processing country. Contact us for current information about hosting, backup, provider, and authorized access locations.

Where international-transfer rules apply, the relevant transfer must have a lawful mechanism and any required safeguards. Depending on the circumstances, this may include an applicable adequacy determination, the UK International Data Transfer Agreement, or the UK Addendum to the EU Standard Contractual Clauses, together with required assessments and protections. Contact our privacy team for information or a copy of safeguards applicable to your information, subject to appropriate redactions. This policy does not itself establish a transfer mechanism or replace a required data processing agreement.

Privacy rights and requests

Depending on your location, the information, and applicable law, you may have rights to know or access personal information; correct it; delete it; receive a portable copy; restrict or object to processing; withdraw consent; limit certain uses of sensitive information; or opt out of sale, sharing, targeted advertising, and certain profiling or automated decisions. Exceptions may apply, including legal retention and protection of other people's information. We do not unlawfully discriminate for exercising privacy rights.

Email privacy@credentialingagents.com or write to the address below. Please describe your request and, for a credentialing file, identify the staffing company or healthcare organization involved. Do not include sensitive documents in the initial email. We may request proportionate information to verify identity or authority, and an authorized agent may submit a request where permitted. We respond within applicable legal deadlines and explain permitted extensions or denials.

When we process records for a client, we generally forward or assist with the request and act on that client's lawful instructions. You may also contact the client directly. We will not direct you away from requests concerning processing for which we are independently responsible. Where an appeal right applies, reply to our decision or email our privacy contact with "Privacy appeal"; we will review it and provide the required response and regulator complaint information.

United States. Where applicable state law gives you rights, you may request access, correction, deletion, or a portable copy and opt out of sale, sharing, targeted advertising, or specified profiling. You may also have rights concerning sensitive information and an appeal of a denied request. Credentialing information is not disclosed for advertising; website identifiers and browsing activity may be disclosed to advertising platforms as described above. The information categories, sources, purposes, recipients, and retention criteria are described in this policy. Applicability and exceptions depend on the law, our role, and the information involved.

Canada. Subject to applicable federal or provincial law, you may request access to your information, challenge its accuracy, ask about its use or disclosure, and withdraw consent where consent is the basis for processing. Withdrawal may be subject to legal or contractual restrictions, which we will explain when relevant. You may raise a concern with our privacy contact or complain to the Office of the Privacy Commissioner of Canada or the appropriate provincial privacy regulator.

United Kingdom. Where UK data protection law applies, you may have rights of access, rectification, erasure, restriction, portability, objection, withdrawal of consent, and safeguards concerning significant automated decisions. For processing we control, we rely on legitimate interests in responding to business inquiries, administering client relationships, and protecting

our services; performance of a contract with you or steps you request before it; compliance with legal obligations; and consent where required, including optional website tracking. A contract with an employer does not by itself establish a contract-based lawful basis for processing an individual's information.

For client-controlled records, the client identifies the lawful basis and any additional condition for special-category or criminal-offence information. Any such processing we control also requires its own applicable condition; this policy does not substitute for it. You can object to legitimate-interest processing and withdraw consent without affecting earlier lawful processing. To exercise rights or obtain details of applicable local privacy arrangements, contact privacy@credentialingagents.com. You may complain to the UK Information Commissioner's Office at ico.org.uk/make-a-complaint/.

Children and other services

Our services are intended for adults aged 18 or older and professional and business use. We do not knowingly collect personal information from users or applicants under 18. If you believe a minor's information has been submitted, contact us so we can investigate and arrange appropriate action, including deletion where required.

External websites, client systems, and independent vendors have their own privacy practices. Our policy describes our processing and does not replace their notices.

Updates and contact

We may update this policy to reflect changes in our services or practices. We will update the effective date and provide additional notice of material changes where appropriate or required. Where a new use requires consent, we will obtain it. A policy update does not itself broaden our contractual permissions to use client records.

Privacy contact: privacy@credentialingagents.com

One Wolf Inc. · Credentialing Agents
1211 W 6th St, Ste 600-151
Austin, Texas 78703
United States