

Injury Armour Privacy Notice

Effective from 22 September 2026

This notice explains how Injury Armour Ltd collects, uses, stores and shares personal information about clients, prospective clients and visitors to our website. It covers our clinical, rehabilitation, performance, communication, booking, payment and website activities. It does not cover employee or job-applicant information, which is handled separately.

Injury Armour is responsible for deciding how and why your patient information is used. We use carefully selected technology providers to help us deliver our services, including Cliniko, Cliniq Apps, FITR, VALD Hub and Heidi. Their role and the information they handle are explained below.

1 Who we are

Injury Armour Ltd is the controller of the personal information described in this notice.

- Legal name: Injury Armour Ltd
- Company number: 14100171
- Registered office: 13 Ellerhayes, Hele, Exeter, England, EX5 4PU
- Privacy contact and postal address: Adam Rutter, Privacy Lead, Injury Armour Taunton, Veritas Park, Hyde Lane, Bathpool, Taunton, TA2 8BU
- Email: info@injuryarmour.com
- Telephone: 0330 043 6448
- ICO registration number: ZB872163

Adam Rutter is our privacy lead. We do not describe this role as a statutory Data Protection Officer unless the legal requirements for appointing one apply.

2 The information we collect

The information we collect depends on how you interact with us and the services you receive. It may include:

- Identity and contact details, including your name, date of birth, address, email address, telephone number, gender where relevant, and emergency contact details.
- Appointment and administrative information, including bookings, attendance, cancellations, correspondence, forms and communication preferences.
- Health information, including symptoms, medical and injury history, diagnoses, medications, allergies, treatment notes, consent records, clinical correspondence, rehabilitation progress and information relevant to safe care.
- Physical and performance information, including strength, movement, force, balance and other test results collected through VALD equipment and associated software.
- Exercise and rehabilitation information, including programmes, completion data, feedback, messages, videos or files supplied through FITR or other agreed channels.
- Referral and funding information, including GP, consultant, insurer, employer, school, sports club or other referrer details, policy or claim information and authorised reports.
- Payment and transaction information. We receive payment status and transaction details but do not retain complete card details. Stripe retains the payment method used for recurring performance-membership subscriptions.
- Telephone and digital communication information, including recorded calls, AI-generated call transcripts, online forms, emails and messages.

- Consultation transcription information where Heidi is used to create a draft clinical note for review by the clinician.
- Marketing choices and, where you have agreed, photographs, videos, testimonials or case-study information.
- Website and device information, including IP address, browser and device information, pages viewed, referring website, cookie choices and analytics information.

3 Where information comes from

We normally collect information directly from you, including when you contact us, speak with our AI receptionist, submit a form, book online, attend an appointment, use a rehabilitation programme, complete testing, make a payment or subscribe to communications.

We may also receive information from a parent, guardian or carer; a GP, consultant or other healthcare professional; an insurer; an employer or corporate client; a school; a sports club or governing body; or another person or organisation that you have authorised or that has a lawful reason to provide it. We may generate information during your assessment, treatment, rehabilitation and testing.

4 Why we use information and our lawful bases

UK data-protection law requires us to have a lawful basis under Article 6 of the UK GDPR whenever we process personal information. Health information is special-category data and requires an additional condition under Article 9. The bases that normally apply are summarised below.

Purpose	Article 6 basis	Article 9 condition when health data is involved
Enquiries, booking and providing requested services	Contract or steps requested before entering a contract. Legitimate interests may apply to efficient administration and responding to enquiries.	Health or social care where health information is needed.
Assessment, diagnosis, treatment, rehabilitation and clinical records	Contract and our legitimate interests in delivering safe, effective and accountable healthcare.	Health or social care under Article 9(2)(h), together with applicable UK law and professional confidentiality.
Performance testing and exercise programming	Contract and legitimate interests in delivering, monitoring and improving the service requested.	Health or social care where the results relate to health; explicit consent where information is used for an optional separate purpose.
Appointment reminders, service messages and AI reception	Contract and legitimate interests in operating our clinics, managing appointments and responding consistently.	Health or social care where a call, form or message contains health information.
Payments, subscriptions, invoicing, tax and accounting	Contract; legal obligation; and legitimate interests in collecting fees, preventing fraud and maintaining accurate accounts.	Normally not applicable. Health or legal-claims conditions may apply if a billing dispute includes clinical information.
Reports and communication with authorised clinicians, insurers or other third parties	Contract, legitimate interests, legal obligation, vital interests or consent, depending on the circumstances.	Health or social care, legal claims, vital interests or explicit consent, depending on the disclosure.

Purpose	Article 6 basis	Article 9 condition when health data is involved
Quality, safety, complaints and legal claims	Legitimate interests in clinical governance, improving services, responding to concerns and establishing or defending legal rights; legal obligation where applicable.	Health or social care and the establishment, exercise or defence of legal claims.
Marketing communications	Consent, or legitimate interests where electronic marketing rules permit a soft opt-in. You can opt out at any time.	We do not use health information for marketing without explicit consent.
Photographs, videos, testimonials and case studies	Consent, which can be withdrawn for future use.	Explicit consent where the material reveals health information.
Website operation, security and analytics	Legitimate interests for security and strictly necessary functions. Consent for non-essential cookies and analytics.	Normally not applicable.
Safeguarding, emergencies and legal disclosures	Legal obligation, vital interests, public task where applicable, or legitimate interests in protecting people and legal rights.	Vital interests, health or social care, substantial public interest or legal claims, as applicable.

Consent to treatment is an important clinical and professional requirement, but it is not necessarily the data-protection basis on which we keep a clinical record. Where we rely on consent for a separate activity, such as marketing or publication of a photograph, you may withdraw that consent at any time. Withdrawal does not affect processing that was lawful before withdrawal.

5 Cliniko and our clinical records

We use Cliniko, provided by Red Guava Pty Ltd, as our principal practice-management and online-booking system. Cliniko is used to manage contact details, appointments, patient forms, clinical notes, correspondence, invoices and related administration.

Injury Armour is the controller of patient information held in our Cliniko account. Red Guava generally acts as our processor and handles that information on our instructions under its terms and UK Data Processing Addendum. Cliniko may use approved subprocessors to provide hosting, backup, communications, support and related services. Requests concerning Injury Armour clinical records should be directed to us using the contact details in section 1.

Further information is available in the [Cliniko Privacy Policy](#) and [Cliniko UK Data Processing Addendum](#).

6 AI receptionist, recorded calls and forms

We use Cliniq Apps, operated by Exiron (Aust) Pty Ltd, for AI-assisted reception, telephone handling, patient forms, communications and related administrative functions. The service can access and update information in Cliniko where required to book, change or cancel appointments and to keep records accurate.

When the AI receptionist answers a call, callers are told that they are interacting with AI and that the call is recorded. The service may collect identity and contact details, appointment information and medical information that the caller chooses to provide. Online or pre-appointment forms may also collect health information and synchronise it into Cliniko.

Recordings and transcripts are used to respond to the caller, create an accurate message or booking record, support quality assurance, investigate concerns and protect clients and staff. They are not used to make automated clinical or treatment decisions. Access is limited to authorised people who need it for these purposes.

Cliniq Apps does not currently publish a fixed automatic deletion period specifically for call recordings or associated transcripts. Its privacy policy states that patient information is retained while we use the service and afterwards until deletion is requested by the patient or by us. We are seeking written confirmation of the precise retention arrangements for recordings and transcripts. Information transferred into Cliniko as part of the clinical record follows the clinical-record retention period.

Cliniq Apps stores patient information on servers in Australia. See the [Cliniq Apps Privacy Policy](#) for more information.

7 Heidi AI clinical documentation

A clinician may use Heidi as an AI-assisted documentation tool during a consultation. Heidi converts the consultation into a draft transcript or clinical note. The clinician remains responsible for checking, correcting and approving the final record before it is placed in Cliniko. Heidi is not used to diagnose you or make treatment decisions without human review.

We will make you aware when Heidi is being used. Live consultation audio is processed in real time and is not retained as an audio recording by Heidi. Draft transcripts and notes are retained only for the period configured by us, up to a maximum of 90 days, and should be deleted after the checked record has been transferred to Cliniko. Heidi states that UK customer information is stored in the UK and processed within the UK or EEA and that patient data is not used to train its AI models.

Further information is available in the [Heidi Health Privacy Policy](#) and [Heidi UK GDPR information](#).

8 Service providers and other recipients

We use the following principal services. The information made available to each provider is limited to what is reasonably required for its function. Depending on its service and legal obligations, a provider may act as our processor, as a separate controller, or in both roles for different activities.

Provider or recipient	How it supports Injury Armour
Cliniko Red Guava Pty Ltd	Practice management, online booking, patient forms, appointments, clinical records, communications and invoicing.
Cliniq Apps Exiron (Aust) Pty Ltd	Recorded AI receptionist calls, booking administration, patient forms, communications and synchronisation with Cliniko.
FITR	Exercise, rehabilitation and performance programming; programme delivery; progress, messages and client feedback.
VALD Hub VALD Pty Ltd	Storage and analysis of strength, movement, force, balance and other physical or performance test results.
Heidi Health	Real-time transcription and generation of draft clinical notes for clinician review.

Provider or recipient	How it supports Injury Armour
Dojo and Stripe	Secure card-payment processing. Stripe also retains payment methods for recurring performance-membership subscriptions. We do not retain complete card details.
Microsoft Outlook and OneDrive	Business email, correspondence and secure business file storage.
QuickBooks	Accounts, invoices, transaction records, bookkeeping and financial reporting.
Mailchimp	Marketing mailing lists, consent records, email campaigns, delivery reporting and unsubscribes.
Website, hosting, analytics and IT providers	Operating, securing and maintaining our website and IT systems; receiving contact forms; managing cookies; measuring website use where consent has been provided.
Professional advisers and authorities	Accountants, lawyers, insurers, regulators, law-enforcement bodies, courts and other authorities where necessary and lawful.

We do not sell personal information. We do not upload client lists to social-media or advertising platforms for targeted advertising.

9 Clinical disclosures and insurers

With your consent or another appropriate legal basis, we may disclose relevant information to GPs, consultants, other healthcare professionals, insurers, employers, corporate clients, schools, sports clubs, governing bodies, parents, guardians or carers. We share only information that is relevant and proportionate to the purpose.

We may communicate with insurers about authorisation, attendance, reports, invoices and claims. The insurer may be a separate controller and will process information under its own privacy notice. Where an employer, school or sports organisation funds a service, we will explain what information is expected to be shared. We will not routinely provide detailed clinical information merely because another organisation is paying for treatment.

We may disclose information without consent where required or permitted by law, including for safeguarding, prevention or detection of serious crime, a court order, regulatory duties, vital interests, or the establishment, exercise or defence of legal claims.

10 International transfers

Injury Armour provides its services in the United Kingdom and does not undertake overseas work. However, some of the technology suppliers we use are based outside the UK or use overseas subprocessors. This means personal information may be processed outside the UK even though your care and our services are provided in the UK. In particular, Cliniko, Cliniq Apps and VALD have Australian operations, while international technology, payment, finance and marketing providers may process information in the EEA, Australia, the United States or other locations.

Where a restricted transfer occurs, we require an appropriate safeguard unless a UK adequacy regulation or another lawful exception applies. Safeguards may include the UK International Data Transfer Agreement, the UK Addendum to approved standard contractual clauses, contractual security and confidentiality requirements, and a transfer risk assessment. You may contact us for more information about the safeguard relevant to a particular provider.

11 How long we keep information

We keep identifiable information only for as long as it is reasonably needed for the purposes described in this notice, including clinical care, professional accountability, legal claims, insurance and financial obligations. Our normal periods are:

Type of information	Normal retention period
Adult clinical records	Eight years after the last appointment or clinical entry.
Children's clinical records	Until the client's 25th birthday, or 26th birthday if treatment ended when the client was 17.
Clinically relevant FITR and VALD information	As part of, or alongside, the clinical record for the applicable adult or child period.
Cliniq Apps call recordings and transcripts	No fixed automatic period is currently confirmed. Cliniq Apps states that patient information is retained while we use the service and afterwards until deletion is requested by the patient or by us. Relevant content added to Cliniko follows the clinical-record period.
Heidi sessions	Live audio is not retained. Draft transcripts and notes are deleted after transfer and checking, and in any event within the configured period of no more than 90 days.
Financial, invoice and transaction records	Six years after the end of the relevant financial year, or longer where required by law or an active dispute.
Stripe subscription information	For the duration of the subscription and thereafter as required for accounting, disputes, fraud prevention and Stripe's legal obligations.
Enquiries that do not become clients	Normally 12 months after the last meaningful contact.
Routine administrative correspondence	Normally up to two years after it is no longer required. Clinically relevant correspondence is retained with the clinical record.
Marketing records	Until consent is withdrawn or you opt out. We may retain a minimal suppression record for as long as necessary to ensure that we respect the opt-out.
Photographs, videos, testimonials and case studies	For the agreed use until consent is withdrawn or the material is no longer required. Continued use is reviewed at least every two years.
Complaints, incidents and legal matters	For the life of the matter and the applicable legal or insurance limitation period.
Website cookies and analytics	For the periods shown in our cookie preference tool, which reflects the technologies currently in use.

A record may be kept longer where there is a legal, safeguarding, insurance or professional reason. Deletion from live systems and encrypted backups may occur at different times, but backup information is protected and removed through the provider's normal deletion cycle.

12 Marketing and photographs

We use Mailchimp and, where appropriate, our communication systems to send news, service updates and promotional material. Marketing is separate from appointment reminders and messages necessary to provide a service. We use consent or another basis permitted by electronic-marketing law, such as the soft opt-in for similar services where its conditions are met.

Every marketing email provides an unsubscribe option. You can also opt out by contacting us. Opting out of marketing will not stop necessary appointment, payment, safety or treatment communications.

We use identifiable photographs, videos, testimonials or case studies only for the agreed purpose and with consent. Refusing or withdrawing this consent will not affect your care. Withdrawal applies to future use; it may not be possible to recall printed material already distributed or third-party copies of material lawfully published before withdrawal.

13 Children and young people

We provide services to children and young people and may process their contact, health, testing and rehabilitation information. Information may be provided by the child, a parent or guardian, a referrer or another person involved in their care.

We provide privacy information in a way appropriate to the child's age and understanding. Depending on age, capacity, confidentiality and safeguarding considerations, rights may be exercised by the young person, a person with parental responsibility, or both. We do not automatically disclose all information to a parent or another paying party where the young person has an applicable right to confidentiality.

14 Security

We use proportionate technical and organisational measures designed to protect personal information against accidental loss, destruction, alteration, unauthorised disclosure or access. These measures include controlled user access, confidentiality obligations, staff training, secure cloud services, password and device controls, multi-factor authentication where available, secure backups and procedures for handling incidents and rights requests.

No method of transmission or storage is completely risk-free. If a personal-data breach occurs, we will assess it and notify the Information Commissioner's Office and affected individuals where the law requires this.

15 Cookies and website technologies

Our website uses cookies and similar technologies. Strictly necessary technologies may operate without consent where they are required to provide or secure a service requested by you. Analytics, advertising and other non-essential technologies are used only after the required consent has been provided through our cookie banner.

The cookie preference tool provides the current list of cookies, their providers, purposes and durations and allows you to accept, reject or change your choices. Refusing non-essential cookies will not prevent you from accessing the essential parts of the website. Embedded services, such as maps or video, may set their own cookies when enabled.

16 Your data-protection rights

Depending on the circumstances, you may have the right to:

- be informed about how your personal information is used;

- request access to your personal information;
- ask us to correct incomplete or inaccurate information;
- ask us to erase information where there is no lawful reason to keep it;
- ask us to restrict how information is used;
- object to processing based on legitimate interests and object at any time to direct marketing;
- receive information you provided in a portable format where the right applies;
- withdraw consent where processing relies on consent; and
- challenge a qualifying solely automated decision. Injury Armour does not currently make decisions producing legal or similarly significant effects solely by automated means.

These rights are not absolute. For example, we may need to retain a clinical record despite an erasure request to meet professional obligations or establish or defend legal claims.

To exercise a right, contact our privacy lead using the details in section 1. We may need to verify your identity. We normally respond within one month, although the law permits an extension for particularly complex or numerous requests. We do not normally charge a fee, but the law allows a reasonable fee or refusal in limited circumstances involving manifestly unfounded or excessive requests.

17 Concerns and complaints

Please contact our privacy lead first if you have a question or concern. We will investigate and try to resolve it promptly.

You also have the right to complain to the Information Commissioner's Office. Visit ico.org.uk/make-a-complaint or telephone 0303 123 1113. Complaining to us first does not affect your right to contact the ICO.

18 Other websites and provider notices

Our website and communications may link to services operated by other organisations. Their own privacy notices explain processing for which they are independently responsible. Linking to another organisation's notice does not transfer Injury Armour's responsibilities for the information we control.

19 Changes to this notice

We review this notice periodically and whenever our services, systems or legal obligations materially change. The latest version will be published on our website with its effective date. Where a change would have a significant effect on how we use existing information, we will take reasonable steps to bring it to the attention of affected people before the new use begins.

Last reviewed: 22 September 2026