NORTHCOTE HEALTH SERVICES LTD

59 Webbs Road, Battersea, London SW11 6RX | Company No. 7060299

GDPR DATA PROCESSING MAP

Data Controller	Northcote Health Services Ltd	Company No. 7060299
Responsible Director	Dr Delphine Sailly	delphine@northcotechiropractic.co.uk
Document version	v3.0 — Updated March 2025	(Previous review: December 2019)
Next review due	March 2027	Annual review required

1. Overview and Scope

This document sets out how Northcote Health Services Ltd (trading as Northcote Chiropractic) collects, processes, stores, and disposes of personal data. It constitutes our Record of Processing Activities (ROPA) as required under Article 30 of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This map covers two categories of data subject: patients (including children) and employees / associates.

2. Lawful Basis for Processing

Under UK GDPR, we must identify a lawful basis before processing personal data. For special category data (health information), an additional condition is required.

Data Category	Lawful Basis (Art. 6)	Special Category Condition (Art. 9)	Notes
Patient health & clinical records	Contract / Legitimate interests	Art. 9(2)(h) — healthcare provision	Core clinical care
Patient contact details	Contract	N/A	Booking and communication
Patient marketing (Mailchimp)	Consent	N/A	Opt-in required; unsubscribe honoured
Patient insurance data	Contract / Legal obligation	Art. 9(Can you be quick2)(h)	For insurance billing via Healthcode
Employee personal data	Contract / Legal obligation	N/A	Payroll, HR, right to work
Employee health data (if disclosed)	Legal obligation / Consent	Art. 9(2)(b) — employment law	e.g. fit notes, reasonable adjustments
DBS check results	Legal obligation	Art. 9(2)(b)	Enhanced DBS; retained per DBS guidance
CCTV (if applicable)	Legitimate interests	N/A	Signage required if in use

3. Data Collected

3a. Patient Data

Collected at first contact and first appointment:

- Full name
- Date of birth
- Address
- Gender
- Phone number and email address
- Medical insurance provider and membership number
- Emergency contact / next of kin
- Full health history and medical records
- X-ray / MRI results (where applicable)
- SF-36 health survey responses
- Scan data (thermal, sEMG, HRV, posture images) via myInsight

No payment card details are ever retained. If card details are taken over the phone, they are destroyed immediately after the transaction is processed.

3b. Employee and Associate Data

Collected during recruitment and onboarding:

- Full name, address, date of birth
- Phone number and email address
- Gender
- National Insurance number
- Bank account details (for payroll)
- Right to work documentation
- CV, covering letter, references
- Enhanced DBS certificate
- GCC registration number (associates)
- Professional indemnity insurance certificate (associates)
- Emergency contact / next of kin
- Payroll and tax information (HMRC starter checklist)

4. How Data Flows Through the Practice

The following describes the journey of patient data from first contact through ongoing care:

Step	Action	System / Location	Who Has Access
1	Patient contacts practice to book	Phone / online booking form	Front desk CAs
2	Basic details captured for appointment	Practice Hub (patient management system)	All staff via individual login
3	Patient attends initial consultation — digital intake form completed on Practice Hub	Practice Hub	Chiropractors + front desk
4	Scan performed at initial consultation	myInsight (name + DOB only)	Front desk + chiropractors
5	Scan results uploaded to patient file	Practice Hub	Chiropractors + front desk
6	Exercise / home care instructions sent	Physitrack (synced from Practice Hub)	Chiropractors + front desk

7	Insurance billing (where applicable)	Healthcode (third-party billing platform)	Front desk + practice director
8	Marketing communications (opt-in only)	Mailchimp	Front desk
9	X-ray referral (with written consent)	Battersea & Wandsworth Chiropractors	Referring chiropractor only
10	Internal admin / payroll records	Google Workspace (email/Drive) + HTA Advisory (payroll)	Director + designated CA

5. Systems and Third-Party Processors

The following systems are used to process personal data. All third-party processors are required to comply with UK GDPR as data processors acting on our instruction.

System	Purpose	Data Held	Access / Notes
Practice Hub	Patient CRM, scheduling, invoicing	Full patient record	All staff via individual login. Passwords changed every 6 months (January & June).
myInsight	Neurological scan software	Name + DOB only	Front desk + chiropractors. Password-protected.
Physitrack	Exercise prescription & patient comms	Synced from Practice Hub	Front desk + chiropractors
Healthcode	Private insurance billing	Name, DOB, diagnosis codes, insurance details	Front desk + director only
Mailchimp	Email marketing (opt-in only)	Name + email	Front desk. Unsubscribes processed immediately.
Google Workspace	Email, internal documents	Staff data, some patient correspondence	Director + designated staff. 2FA enabled.
HTA Advisory	Payroll processing	Staff payroll data	Director only. Acts as data processor.
iMessage / SMS	Patient appointment reminders	Name + phone number	Front desk + chiropractors via Cliniko automations
Excel / Google Sheets	Cashflow, scheduling	Financial data; no patient health data	Front desk + director

6. Access Controls

Access to personal data is restricted on a need-to-know basis:

Role	Systems Accessible
Company Director (Dr Sailly)	All systems — full access
Chiropractors	Practice Hub, myInsight, Physitrack, iMessage/SMS

Front Desk CAs	Practice Hub, myInsight, Physitrack, Healthcode, Mailchimp, iMessage/SMS
Payroll provider (HTA Advisory)	Staff payroll data only — acts as data processor
External marketing consultant	Mailchimp only — no access to clinical or patient records
Third-party referral (e.g. X-ray)	Specific patient data only, with written patient consent

All system passwords are changed every 6 months (January and June). Staff who leave the practice are deactivated from all systems on their final day of work.

7. Data Retention and Disposal

Data Type	Retention Period	Basis	Disposal Method
Adult patient clinical records	8 years from last treatment	GCC / professional guidance	Secure electronic deletion from Practice Hub
Paediatric patient records (under 18 at treatment)	Until patient's 25th birthday (or 26th if treatment ended near 18th birthday)	NHS / professional body guidance	Secure electronic deletion
Physical intake forms (legacy only)	Practice is now fully digital. Any legacy paper forms should be shredded if not already done.	Minimisation principle	Confidential shredding (First Mile or equivalent)
Employee personal records	6 years after employment ceases	Employment law	Secure deletion / shredding
Payroll records	6 years	HMRC requirement	Secure deletion via HTA Advisory
DBS certificates	Retained only as long as necessary — record of check date kept	DBS Code of Practice	Secure deletion; do not retain certificate
Job applications (unsuccessful)	3 months after recruitment process ends	Minimisation principle	Secure deletion
CCTV footage (if applicable)	30 days	ICO guidance	Automatic overwrite

8. Data Subject Rights

Under UK GDPR, all data subjects have the following rights. Requests should be directed to Dr Delphine Sailly at del@northcotechiropractic.co.uk and must be responded to within one calendar month.

- Right of access — patients and staff may request a copy of all data held about them
- Right to rectification — inaccurate data must be corrected promptly
- Right to erasure ('right to be forgotten') — subject to retention obligations above

- Right to restriction of processing
- Right to data portability (electronic records)
- Right to object to processing for marketing purposes
- Right to withdraw consent (where consent is the lawful basis — e.g. Mailchimp marketing)

Requests will be logged with the date received, action taken, and date responded. A template response is available from the Director.

9. Data Breach Procedure

A personal data breach must be reported to the ICO within 72 hours if it is likely to result in a risk to individuals' rights and freedoms. All staff must report any suspected breach to Dr Delphine Sailly immediately.

A breach includes: loss of a device containing patient data, accidental email to wrong recipient, unauthorised access to Practice Hub, or sending patient data to an incorrect third party.

The ICO can be contacted at: ico.org.uk | 0303 123 1113

10. Review and Accountability

This document must be reviewed annually, or immediately following any of the following:

- A change in the systems used to process data
- A data breach or near-miss
- A change in the law or ICO guidance
- A significant change to the practice (e.g. new staff, new services, change of ownership)

Review Date	Reviewed By	Changes Made
December 2019	Dr Emma Burniston	Original version
March 2026	Dr Delphine Sailly	Major update: new ownership, system changes (Practice Hub, Healthcode), lawful basis added, retention periods corrected for paediatrics, breach procedure added
March 2026 (due)		

Approved by: Signed: _____ Dr Delphine Sailly, Company Director Date: _____	