

Cohort Science Ltd

Privacy Notice

Effective Date: 23 July 2026

This Privacy Notice explains how Cohort Science Ltd (“Cohort Science”, “we”, “us” or “our”) collects, uses, stores, shares and protects personal information, including health information, in connection with our websites, applications and research activities.

It is designed to cover both United Kingdom (UK GDPR) and United States (including HIPAA where applicable) requirements in clear language.

1. Who we are

Cohort Science Ltd is a company registered in England and Wales (Company No. 13780369), with its registered office at 15 Stukeley Street, London, WC2B 5LT, United Kingdom. We are the sponsor of research registries such as AccessALL, AccessBrainHealth and other ACCESS studies.

uMed Technologies Inc (Delaware, USA) provides operational and technical support services in the United States. Both Cohort Science Ltd and uMed Technologies Inc are subsidiaries of Umedeor Ltd.

For the purposes of UK data protection law, Cohort Science Ltd is the data controller for the personal data we process as study sponsor. For certain US activities involving Protected Health Information (PHI), we act in accordance with HIPAA and applicable Business Associate arrangements.

2. Scope of this Notice

This Notice applies to:

- visitors to our websites;
- individuals who use our patient-facing applications;
- participants (or potential participants) in our research registries and studies; and
- individuals who contact us or otherwise interact with us.

3. Information we collect

Depending on how you interact with us, we may collect:

- **Identity and contact data** – name, date of birth, address, email, telephone number, and similar details;
- **Health and medical data** – information from your medical records, questionnaires, patient-reported outcomes, and other health-related information you or your healthcare provider share with us (this is special category / PHI data);
- **Technical and usage data** – IP address, device information, browser type, pages visited, and cookie identifiers;
- **Communications data** – records of emails, SMS, phone calls and other correspondence with us.

4. How we use your information

We use personal information for the following purposes:

- to operate our websites and applications;
- to invite eligible individuals to participate in research registries and studies (where permitted);
- to administer research studies and registries, including linking clinical data with patient-reported information;
- to communicate with you about studies you have joined or expressed interest in;
- to meet our legal, regulatory and ethical obligations (including safety reporting);
- to improve our services and websites; and
- to protect our rights, property and safety, and those of others.

5. Legal bases for processing (UK / EEA)

Where UK GDPR or equivalent laws apply, we rely on one or more of the following bases:

- **Consent** – for example when you agree to participate in a study or to receive certain communications;

- **Legitimate interests** – for example operating our websites, ensuring security, and conducting research in the public interest where appropriate safeguards are in place;
- **Legal obligation** – where we must process data to comply with law; and
- **Public interest / scientific research** – for certain research activities with appropriate safeguards under Article 9(2)(j) and Article 89 UK GDPR.

For special category (health) data we additionally rely on explicit consent or the research condition with safeguards, as applicable.

6. United States – Health information (HIPAA)

Where we receive Protected Health Information (PHI) from US healthcare providers or through patient authorisation:

- we handle that information in accordance with the HIPAA Privacy and Security Rules and applicable Business Associate Agreements;
- we only use and disclose PHI as permitted by your authorisation, the relevant study protocol, or as otherwise allowed or required by law; and
- we apply the minimum necessary standard.

7. Who we share information with

We may share personal information with:

- service providers and processors who support our operations (under appropriate contracts);
- research collaborators, academic institutions and life sciences companies under data sharing agreements (usually with de-identified or pseudonymised data);
- regulators, ethics committees, and other authorities where required;
- professional advisers; and
- a buyer or successor in the event of a reorganisation or sale of assets.

We do not sell your personal or health information.

8. International transfers and data location

Health information collected from users in the United States is stored on servers located in the United States (currently Amazon Web Services – US regions).

Health information collected from users in the United Kingdom is stored on servers located in the United Kingdom or the European Economic Area.

Where we transfer personal data internationally, we do so only where permitted by law and with appropriate safeguards (such as Standard Contractual Clauses or other approved mechanisms).

9. How long we keep information

We retain personal information only for as long as necessary for the purposes described in this Notice, including to meet legal, regulatory, research, and accountability requirements. Retention periods for research data are typically set out in the relevant study protocol and consent materials and may extend for many years after the end of a study.

10. Your rights

UK / EEA rights

Depending on your location you may have the right to:

- access your personal data;
- rectify inaccurate data;
- request erasure (in certain circumstances);
- restrict or object to processing;
- data portability; and
- withdraw consent where we rely on consent.

You also have the right to lodge a complaint with the UK Information Commissioner's Office (ICO) or your local supervisory authority.

US rights (including California)

Depending on your state of residence you may have additional rights regarding access, correction, deletion, and certain disclosures of personal information. California residents may contact us to request information about disclosures of personal information for direct marketing purposes (we do not sell personal information).

11. Security

We implement appropriate technical and organisational measures to protect personal information, including encryption, access controls, and staff training. We are certified to ISO 27001 and hold Cyber Essentials Plus certification. No method of transmission or storage is completely secure, and we cannot guarantee absolute security.

12. SMS / Text messaging

If you consent to receive text messages from us:

- messages may relate to study information, questionnaires, or opportunities to take part in further research;
- message frequency varies; message and data rates may apply;
- you can opt out at any time by replying STOP;
- text messages may not be encrypted – please protect your device.

Full details of our SMS messaging terms are set out in our SMS Terms & Conditions

13. Children

Our websites and primary registries are not directed at children under 18. We do not knowingly collect personal information from children without appropriate parental or guardian consent where required by law.

14. Changes to this Notice

We may update this Privacy Notice from time to time. The latest version will always be available on our website. Material changes will be communicated in an appropriate manner.

15. Contact us

If you have questions about this Privacy Notice or wish to exercise your rights, please contact:

Data Protection Officer (UK)

Email: dpo@cohort.science

Phone (UK): +44 (0) 808 304 9869

Privacy Officer (US)

Email: privacyofficer@cohort.science

Phone (US): +1 888 454 5580

Postal: Cohort Science Ltd, 15 Stukeley Street, London, WC2B 5LT, United Kingdom