

Privacy Notice

Clinical Assurance Solutions Ltd

Version: 1.0

Effective Date: 21 September 2026

Last Reviewed: 21 September 2026

Introduction

This privacy notice explains how Clinical Assurance Solutions Ltd collects, uses, stores and protects personal information when providing clinical safety, digital health assurance, compliance and consultancy services.

We are committed to protecting personal information and processing it fairly, lawfully and transparently in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable legislation.

Clinical Assurance Solutions Ltd is the data controller for the personal information described in this notice.

Contact Details

Clinical Assurance Solutions Ltd

Telephone: 07876 566665

Email: steve@clinicalassurancesolutions.co.uk

Company Number: 17299593

What Information We Collect

We may collect and use the following categories of personal information.

Client and Business Contact Information

- Name
- Job title
- Organisation name
- Business address
- Business email address

- Business telephone number
- Correspondence and communications
- Records of meetings and decisions

Contract and Project Information

- Client account records
- Engagement documentation
- Assurance records
- Project information
- Contractual information
- Service history
- Records of decisions and recommendations

Financial Information

- Invoicing information
- Payment records
- Transaction information

Website Information

Where relevant, we may collect limited technical information relating to the use of our website, including:

- IP address
- Device information
- Browser information
- Website usage information

Personal Information Encountered During Assurance Activities

Clinical Assurance Solutions Ltd does not provide healthcare services and does not routinely collect, maintain or manage patient records.

However, during clinical safety, assurance, audit and compliance assessments of digital health systems, personal information, including special category health information, may occasionally be visible within client-owned systems.

Such access is incidental to the provision of contracted services and is limited to what is necessary to fulfil our professional obligations.

We do not routinely extract, copy, create separate records from, or retain patient information unless this is specifically required as part of an agreed engagement or to support documented assurance activities.

Where special category personal information is encountered during assurance work, appropriate technical, organisational and confidentiality safeguards are applied.

Why We Collect and Use Personal Information

Providing Professional Services

We collect and use personal information to:

- Deliver Clinical Safety Officer services
- Conduct DCB0129 and DCB0160 assurance activities
- Perform audits, reviews and assessments
- Deliver consultancy and advisory services
- Manage projects and engagements
- Communicate with clients
- Produce reports and recommendations
- Improve the quality of our services

Lawful Bases

Contract

Processing is necessary to enter into and perform contracts with our clients.

Legitimate Interests

We process client contact and project-related information to provide clinical safety, assurance and compliance services for digital health technologies.

This enables us to:

- Plan and deliver assessments
- Maintain communication with clients
- Manage contractual relationships

- Produce assurance outputs
- Maintain professional records
- Improve the quality and effectiveness of our services

This processing supports the development, deployment and ongoing assurance of safe and effective digital health technologies.

We only process information that is necessary for these purposes and have concluded that our legitimate interests do not override the rights and freedoms of the individuals concerned.

Compliance With Legal and Regulatory Obligations

We may process personal information where necessary to comply with:

- Tax and accounting legislation
- Regulatory obligations
- Legal proceedings
- Court orders
- Requests from competent authorities
- Professional obligations

Lawful Basis

Legal Obligation

Processing is necessary to comply with applicable laws and regulatory requirements.

Queries, Complaints and Claims

We may process personal information in order to:

- Respond to enquiries
- Investigate complaints
- Handle disputes
- Manage professional indemnity matters
- Establish, exercise or defend legal claims

Lawful Bases

Legitimate Interests

It is in our legitimate interests to maintain service quality, investigate concerns and protect the interests of clients, individuals and the business.

Legal Obligation

In some circumstances we may be required by law or regulation to process information relating to complaints, disputes or claims.

Where We Obtain Personal Information

We may obtain personal information:

- Directly from clients and prospective clients
- From individuals who contact us
- From publicly available sources
- From professional networking services such as LinkedIn
- From client organisations as part of an engagement
- Through documentation provided to support assurance activities

Client organisations may provide information about relevant staff, project personnel, stakeholders and system contacts where necessary to deliver contracted services.

How Long We Keep Information

We retain information only for as long as necessary to fulfil the purposes for which it was collected.

Typically:

Client and Contract Records

Client contact information, contracts, correspondence and engagement documentation are generally retained for up to **six years** following the completion of an engagement.

Financial Records

Financial records are retained for the periods required by UK tax and accounting legislation.

Clinical Safety and Assurance Artefacts

Clinical safety documentation and assurance artefacts, including but not limited to:

- Clinical safety reports
- Hazard logs
- Safety cases
- Safety assessments
- Audit and assurance reports
- Review findings
- Workshop outputs
- Supporting evidence

may be retained for up to **six years following completion of an engagement**, unless:

- A longer retention period is agreed contractually;
- A legal or regulatory requirement applies; or
- Retention is necessary for the establishment, exercise or defence of legal claims.

Patient Information

Patient information encountered incidentally during assurance activities is not routinely retained by Clinical Assurance Solutions Ltd.

How We Protect Personal Information

We implement appropriate technical and organisational measures designed to protect personal information against unauthorised access, loss, disclosure, alteration or destruction.

These measures may include:

- Access controls
- Strong authentication and multi-factor authentication where available
- Secure cloud-based services
- Device encryption
- Secure backups
- Confidentiality obligations

- Regular software and security updates
- Appropriate information governance practices

Access to personal information is restricted to those who require it for legitimate business purposes.

Who We Share Information With

We do not sell personal information.

We may share personal information where necessary with the following categories of recipient.

Data Processors

We use trusted third-party providers to support our business operations, including providers of:

- Email services
- Microsoft 365 services
- Cloud storage
- Website hosting
- Business administration systems
- Accounting software

These organisations process information on our behalf and under contractual controls.

Professional Advisers

We may share information with:

- Accountants
- Solicitors
- Tax advisers
- Other professional advisers

where necessary to obtain professional advice.

Insurance Providers

Information may be shared with:

- Professional indemnity insurers

- Insurance brokers
- Claims handlers

where necessary to obtain or manage insurance cover or claims.

Regulatory and Legal Authorities

Where required by law, we may share information with:

- HM Revenue & Customs (HMRC)
 - Courts and tribunals
 - Regulatory bodies
 - Law enforcement agencies
 - Public authorities exercising lawful powers
-

International Transfers

Some of our service providers may process information outside the United Kingdom.

Where personal information is transferred internationally, we ensure that appropriate safeguards are in place, including:

- UK adequacy regulations;
- The UK International Data Transfer Agreement (IDTA); or
- The UK Addendum to the EU Standard Contractual Clauses.

These safeguards are designed to ensure that personal information receives an equivalent level of protection.

Your Data Protection Rights

Under UK data protection law, you may have the right to:

- Request access to your personal information
- Request correction of inaccurate information
- Request erasure of information in certain circumstances
- Request restriction of processing
- Object to processing
- Request data portability where applicable

- Withdraw consent where consent is relied upon

If you wish to exercise any of your rights, please contact us using the details provided above.

How to Complain

If you have any concerns about how we use your personal information, please contact us:

Email: steve@clinicalassurancesolutions.co.uk

We will endeavour to resolve any concerns promptly and fairly.

If you are not satisfied with our response, you may complain to the Information Commissioner's Office (ICO):

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Telephone: 0303 123 1113

Website: www.ico.org.uk
