

Clinical Assurance Solutions Ltd

Data Handling and Confidentiality Statement

Version: 1.0

Effective Date: 21 September 2026

Last Reviewed: 21 September 2026

Purpose

Clinical Assurance Solutions Ltd provides independent Clinical Safety Officer (CSO), digital health assurance, compliance, audit and advisory services to organisations developing, implementing and operating digital health technologies.

This statement describes our approach to handling confidential information, personal information and commercially sensitive information encountered during the delivery of our services.

Commitment to Confidentiality

Clinical Assurance Solutions Ltd recognises the importance of maintaining the confidentiality, integrity and security of information provided by clients.

Information obtained during an engagement is used solely for the purpose of delivering the agreed professional services and is not disclosed to unauthorised parties.

Confidential information includes, but is not limited to:

- Business information
- Commercially sensitive information
- Technical documentation
- System architecture information
- Clinical safety documentation
- Security documentation
- Personal information
- Special category personal information
- Intellectual property

All information is handled in accordance with applicable legal, contractual and professional obligations.

Information We Typically Access

As part of our assurance and consultancy activities, we may access:

- Client contact information
- Project documentation
- Governance records
- Clinical safety documentation
- Technical documentation
- System design information
- Audit evidence
- Risk assessments
- Policies and procedures
- Training and operational records

The specific information accessed will depend upon the nature of the engagement.

Patient Information

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

However, during assessments of digital health systems, patient information and other personal information may occasionally be visible within client systems.

Examples may include:

- User records
- Screenshots
- Test environments
- Live application interfaces
- Clinical workflows
- Audit logs

- Configuration settings
- Clinical safety evidence

Where such information is encountered:

- Access is limited to what is necessary to complete the engagement.
- Information is not viewed unnecessarily.
- Information is not disclosed to unauthorised parties.
- Information is not routinely copied or extracted.
- Information is not routinely retained following completion of the activity.

Clinical Assurance Solutions Ltd applies a principle of minimum necessary access at all times.

Special Category Information

During health and care assurance activities, special category personal information may occasionally be encountered.

Examples include:

- Health information
- Clinical records visible within systems
- Patient-identifiable information present within evidence supplied by clients

Where such information is encountered:

- Access is restricted to authorised activities.
- Information is handled confidentially.
- Processing is minimised wherever possible.
- Information is protected using appropriate technical and organisational controls.

Information Security Controls

Clinical Assurance Solutions Ltd implements appropriate security measures designed to protect information from unauthorised access, loss, disclosure, alteration or destruction.

These measures may include:

- Strong passwords
- Multi-factor authentication
- Device encryption
- Secure cloud storage
- Access controls
- Secure transfer methods
- Regular software updates
- Malware protection
- Secure backup arrangements

Access to information is restricted to authorised individuals who require it for legitimate business purposes.

Storage and Retention

Information is retained only where required for:

- Delivery of contracted services
- Professional record keeping
- Clinical safety assurance records
- Legal or regulatory obligations
- Defence of legal claims

Clinical Assurance Solutions Ltd may retain assurance artefacts and engagement records, including:

- Clinical safety reports
- Hazard logs
- Safety cases
- Review reports
- Audit reports
- Workshop outputs
- Supporting evidence

Retention periods are determined in accordance with contractual, legal and business requirements.

Patient information encountered incidentally during assurance activities is not routinely retained.

Data Sharing

Clinical Assurance Solutions Ltd does not sell personal information.

Information may be shared only where necessary with:

- Approved service providers acting under contractual controls
- Professional advisers
- Insurers
- Regulatory authorities
- Courts or public authorities exercising lawful powers

Information is shared only where there is a legitimate business, contractual or legal requirement to do so.

Working with Client Systems

Where access to client systems is required:

- Access permissions will be limited to those necessary for the engagement.
- Client access controls will be respected.
- Information will only be accessed for authorised purposes.
- Access credentials will be protected appropriately.
- Access will be removed when no longer required.

Any information security concerns identified during an engagement will be reported through appropriate channels.

Professional and Ethical Standards

Clinical Assurance Solutions Ltd operates in accordance with recognised principles of:

- Confidentiality

- Integrity
- Professional competence
- Information governance
- Clinical risk management
- Patient safety

We seek to ensure that information obtained during engagements is handled responsibly and proportionately whilst supporting the safe development and deployment of digital health technologies.

Contact

Questions regarding this statement or our information handling practices may be directed to:

Clinical Assurance Solutions Ltd

Email: steve@clinicalassurancesolutions.co.uk

Telephone: 07876 566665
