



Clinical Guardian

Service Definition For G-Cloud 15

Clinical Guardian Overview

Clinical Guardian is a cloud-hosted Software as a Service (SaaS) solution developed by Applied Healthcare Solutions to support clinical audit and governance activity. It applies a structured methodology for auditing care and is delivered through a web-based application designed with clinical input.

The methodology involves peer review of clinical records based on risk stratification of the clinical workforce, to help governance teams focus audit activity on areas with higher potential for concern. By auditing cases from across an organisation, underlying systemic issues can be identified and reviewed as part of local governance processes.

Clinical Guardian supports organisations to maintain evidence of attention to higher-risk areas, oversight activity, timely review, and the actions taken in response to audit findings. The service is intended to support clinical governance and quality improvement activity; it does not replace an organisation's Electronic Patient Record (EPR) or clinical record system.

The Problem to be addressed

Audit is a vital part of good governance but takes time and effort from stretched resources.

The impact can be a compromised audit regime that reduces consistency and coverage and can affect an organisation's ability to maintain effective oversight.

Cost impacts

- ✓ Manual audit is time consuming.
- ✓ Coverage is limited due to resource constraints.
- ✓ Fewer audits expose greater risk.
- ✓ Where quality issues are not detected and addressed promptly, consequences can have significant operational and financial impact.

Staff Impacts

- ✓ Staff want to perform well but are often overburdened by operational pressures.
- ✓ A small minority of performance concerns can have disproportionate impact.
- ✓ Support audit, early review, and constructive feedback is important for development and assurance.

Care Impacts

- ✓ Patterns of poor behaviour or recurring issues can impact patient safety.
- ✓ Divergence from best practice guidelines impacts outcomes.
- ✓ Without good data and reports, governance issues may be harder to identify and escalate.

How can Clinical Guardian Audit Software Help?

Clinical Guardian uses technology to implement a structured audit methodology. The web-based application guides authorised users through the steps of the audit process to support consistent and efficient review activity. This approach helps governance teams identify cases requiring review and determine appropriate follow-up actions in line with local governance arrangements.

Clinical Guardian is delivered as a fully hosted service. This supports access to the service without the customer needing to install or maintain local infrastructure for the application. Where organisations rely on manual processes, reporting and audit administration can place additional burden on clinical and governance staff; Clinical Guardian is designed to support a more structured workflow and more consistent reporting.

The Clinical Guardian methodology and software application have been designed and built with continuous clinical input, specifically to address the challenges of delivering comprehensive clinical audit in accordance with the compliance requirements of a healthcare provider.

The web-based application is hosted in a secure environment and accessed via any appropriate internet connected device. Auditors can work remotely and whenever time permits, subject to the organisation's own information governance requirements for remote working and device usage. Data is uploaded from electronic record systems and analysed in Clinical Guardian using risk stratification rules across the clinical workforce to help target audit effort where it is most needed.

Immediate Benefits

When Clinical Guardian goes live, three things happen in quite separate ways, each of great importance: **Firstly**, cases of potential concern can be highlighted for review so governance teams can prioritise audit activity and take appropriate follow-up actions in line with local governance processes. Where issues do arise, the service supports the maintenance of an audit record of reviews, findings and outcomes.

Secondly, as the database grows, the reporting tools and focused audits can help identify areas of divergence from local or national guidance. This can inform operational review and quality improvement planning, supporting ongoing refinement of policies, training priorities and ways of working.

Thirdly, from day one, a structured mechanism for feedback and reflective practice can be established. Clinicians may use audit activity to receive feedback, self-refer cases for review where appropriate, and build records that support appraisal and development in line with organisational practice.

In summary, the expected benefits include:

- ✓ More efficient audit workflows that help use governance resources effectively.
- ✓ Improved visibility of audit findings to support patient safety and quality oversight.
- ✓ A supportive and collaborative environment for feedback and learning.
- ✓ Constructive feedback aiding continuous improvement.

Design Standards for Data Security

Clinical Guardian has been developed according to security by design principles, implementing measures governing both physical and logical access to the system, according to best practice and in line with the Department for Health, the wider NHS and HMG requirements.

Information governance aligns with UK GDPR and the Data Protection Act 2018. The Risk Management Framework is implemented according to DCB0129, addressing clinical risk and incorporated into the software development change control process.

The system design gives consideration to security guidelines and regular vulnerability testing during development using tools developed by CREST accredited penetration testers. This helps reduce exposure to common vulnerability classes, for example those referenced in the OWASP Top 10. Adherence to these high standards is supported by regular submissions of the NHS Data Security and Protection Toolkit (ODS Ref. 8JQ68).

Applied Healthcare Solutions is Registered with ICO, Ref: ZA220750

Infrastructure support is certified to ISO 27001 and Cyber Essentials Plus

Clinical Guardian data is encrypted in transport using HTTPS and TLS 1.2. This helps protect information between the hosting facility and the end-user web browser.

No patient attributable information is included in the data extract to ensure the Clinical Guardian database only stores pseudonymised patient records. The databases are hosted on encrypted servers in a commercial facility, providing high security and resilience according to ISO 9001, ISO 27001, and ISO 22301 certifications.

Access to the application requires secure login credentials and functionality is further protected using role-based access controls. This ensures access to sensitive information and functionality is restricted to approved users who have been allocated appropriate role-based permissions.

The system software and data are regularly backed up according to industry best practice, using the latest tools. With the resilience inherent in the hosting environment and the backup regime, the Business Continuity and Disaster Recovery approach is designed to support high availability and timely recovery in the event of an unplanned outage.

Frequent security patches and updates are managed routinely along with response activity triggered where relevant CVE alerts are published.

Onboarding - 6 steps to implementing Clinical Guardian

1. **Book a demo** – the Clinical Guardian team will take you through the key features of the software and the methodology.
2. **Commercial discussion** – the commercial team will confirm how the price model is applied to your service type and ensure the information governance requirements are aligned.
3. **Technical Test** – the technical support team will complete a test to ensure appropriate data connectivity with your clinical system.
4. **Trial Period** – a trial period can be arranged for up to 3 months so that you can be confident Clinical Guardian is right for your organisation
5. **Onboarding Programme** – Your account manager will lead a detailed onboarding programme to train your team and ensure the system is tailored to meet your service needs.
6. **Ongoing Support** – When you go live, our support team continues to give you the support needed to help customers use the service effectively using Clinical Guardian.

Training Methods

Training and onboarding are typically conducted as remote sessions by customer request, using online meetings. Face-to-face training can be arranged by agreement. Training can be delivered for different user groups (for example administrators and auditors) depending on the customer's internal roles and access model. User materials are provided to support "train-the-trainer" so customers can onboard new team members in future

Technical Requirements

As Clinical Guardian is a fully hosted web application, it can be accessed from any compliant, internet connected web browser. This has the advantage that auditors can work remotely without needing to be connected directly to the NHS SPINE. The contract Terms set out clearly each party's responsibilities for data protection and it remains the end user's responsibility to ensure that they access Clinical Guardian from an appropriate location and using a compliant device, so that sensitive data is not compromised. The sensitivity of the case data is limited by virtue of the pseudonymisation of the upload prior to storage in the Clinical Guardian database.

Data is exported from Principal Clinical Systems and converted into a standard format for use within Clinical Guardian. Differences between Principal Clinical system implementations can impact the availability of data in Clinical Guardian.

The data types used to assess a clinician's actions during a patient contact consists of:

- ✓ Demographic information about the patient but no person identifiable data items.
- ✓ Temporal information about the encounter.
- ✓ Clinical information including diagnosis, examination, history, prescriptions, informational outcomes, dispositions, durations, and any notes recorded.
- ✓ A pseudonymised reference ID to link data back to the originating clinical system if required by the provider organisation where follow up is required.

Subscription Fee

The Price Model for Clinical Guardian is provided as a separate document. It describes the capitation-based approach to calculating the licence fee. This is designed to fairly relate the fee to the size of the organisation, which has a direct bearing on the demands placed on the system and the support team at AHS. This model also recognises that broadly healthcare providers are funded according to the size of the patient population they serve. This capitation-based approach provides a single subscription price for using Clinical Guardian. There is no additional fee for premium features, no fee per user, no fee per audit, and no limit on reports run or data exported. The subscription also includes software updates released through the product roadmap, including enhancements delivered in response to customer feedback.

The fee includes initial training. We aim to "train-the-trainer" and provide you with materials to allow you to train new team members when they join in the future. We can also be available to provide additional training by request. Technical support is available during office hours on weekdays. We can be contacted by phone, but the best way is typically to raise a support ticket by email. Support tickets are monitored and progressed in line with the support process.

Clinical Guardian provides a solid and reliable basis for audit and governance aligned to the dynamic care settings now commonplace.

Applied 
Healthcare
Solutions