Clinitalk Risk Management File

for DCB0160 compliance purposes

**Instructions:**

To complete this form, enter your details in the box below.

Review this document annually and update your details.

You can delete this highlighted text

# Change control – Last review date

|  |  |  |
| --- | --- | --- |
| Name | Last Review Date | Comments |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Contents

[2.1 Risk Management process 5](#_Toc157105814)

[2.2 Clinitalk Top Management Commitment 5](#_Toc157105815)

[2.3 Safety Officer 5](#_Toc157105816)

[2.4 Competencies of Personnel 6](#_Toc157105817)

[2.5 Third Party Products 6](#_Toc157105818)

[2.6 Review of risk 6](#_Toc157105819)

[3.0 Project Safety Documentation and Repositories 6](#_Toc157105820)

[3.1 Risk Management File 7](#_Toc157105821)

[3.2 Risk Management Plan 7](#_Toc157105822)

[Definition of the Clinitalk IT system in its use context 7](#_Toc157105823)

[3.2a Relevant procedures, policies and resources required to ensure effective and efficient risk management. 7](#_Toc157105824)

[3.2b Project management processes 8](#_Toc157105825)

[3.2c Clinitalk system development lifecycle 8](#_Toc157105826)

[**Clinitalk Lifecycle and Risk Activities** 8](#_Toc157105827)

[1. Conception and Planning: 8](#_Toc157105828)

[2. Design: 8](#_Toc157105829)

[3. Development: 8](#_Toc157105830)

[4. Testing: 9](#_Toc157105831)

[5. Deployment: 9](#_Toc157105832)

[6. Operations and Maintenance: 9](#_Toc157105833)

[7. Change Management: 9](#_Toc157105834)

[8. End-of-Life (Retirement): 10](#_Toc157105835)

[9. Documentation and Compliance: 10](#_Toc157105836)

[10. Review and Continuous Improvement: 10](#_Toc157105837)

[3.2d Criteria used to estimate risk 10](#_Toc157105838)

[Clinitalk risk severity definitions 10](#_Toc157105839)

[Clinitalk Likelihood categories 11](#_Toc157105840)

[Clinitalk risk matrix 12](#_Toc157105841)

[Clinitalk Risk Acceptability Definitions 12](#_Toc157105842)

[3.2e Risk Activity Roles and Authority 12](#_Toc157105843)

[3.2f Additional resources required 13](#_Toc157105844)

[3.2g Authority 13](#_Toc157105845)

[3.2h Periodicity of review 13](#_Toc157105846)

[3.2i Monitoring and responding to safety incidents 13](#_Toc157105847)

[3.2j The risk management plan review 13](#_Toc157105848)

[3.3 Hazard Log 14](#_Toc157105849)

[Key to the Clinitalk Hazard Log labels 14](#_Toc157105850)

[Safety incident log 15](#_Toc157105851)

[Hazard Log Table 16](#_Toc157105852)

[Hazard Log Screenshots: 21](#_Toc157105853)

[3.5 Safety Case Report 27](#_Toc157105854)

[Introduction to the Safety Case Stages 27](#_Toc157105855)

[Stage 1 – Conception and planning 27](#_Toc157105856)

[Stage 2 – Design 27](#_Toc157105857)

[Stage 3 – Development 27](#_Toc157105858)

[Stage 4 – Testing 27](#_Toc157105859)

[Stage 5 – Deployment 27](#_Toc157105860)

[Stage 6 – Operations and maintenance 27](#_Toc157105861)

[Stage 7 – Change management. 27](#_Toc157105862)

[Stage 8 – End of life (Retirement) 28](#_Toc157105863)

[Stage 9 – Documentation and compliance 28](#_Toc157105864)

[Stage 10 – Review and continuous improvement 28](#_Toc157105865)

[Product description – Safety Case 28](#_Toc157105866)

[Safety Case Reports 28](#_Toc157105867)

[Report - stage 1 - Conception and planning: 28](#_Toc157105868)

[Report - stage 1 - Risk evaluation 32](#_Toc157105869)

[Report - stage 1 – QA and Sign off: 33](#_Toc157105870)

[Report - stage 2 - Design 33](#_Toc157105871)

[Report - stage 2 - Risk evaluation 36](#_Toc157105872)

[Report - stage 2 - QA and Sign off: 37](#_Toc157105873)

[Report - stage 3 - Development 37](#_Toc157105874)

[Report - stage 3 - Risk evaluation 43](#_Toc157105875)

[Report - stage 4 - Testing 43](#_Toc157105876)

[Report - stage 4 - Risk evaluation 46](#_Toc157105877)

[Report - stage 4 - QA and Sign off: 46](#_Toc157105878)

[Report - stage 5 - Deployment 46](#_Toc157105879)

[Report - stage 5 - Risk evaluation 48](#_Toc157105880)

[Report - stage 5 - QA and Sign off: 48](#_Toc157105881)

[Report - stage 6 - Maintenance 48](#_Toc157105882)

[Report - stage 6 - Risk evaluation 50](#_Toc157105883)

[Report - stage 6 - QA and Sign off: 51](#_Toc157105884)

[Report - stage 7 - Change management 51](#_Toc157105885)

[Report - stage 7 - Risk evaluation 51](#_Toc157105886)

[Report - stage 7 - QA and Sign off: 52](#_Toc157105887)

[Report - stage 8 - End of life 52](#_Toc157105888)

[Report - stage 8 - Risk evaluation 55](#_Toc157105889)

[Report - stage 9 - Documentation and compliance 55](#_Toc157105890)

[Report - stage 9 - Risk evaluation 56](#_Toc157105891)

[Report - stage 10 - Review and continuous improvement 56](#_Toc157105892)

[Report - stage 10 - Risk evaluation 57](#_Toc157105893)

[4.1 Clinical risk analysis process 58](#_Toc157105894)

[4.2 Scope Definition 58](#_Toc157105895)

[Scope and intended use: 58](#_Toc157105896)

[Human interface: 58](#_Toc157105897)

[4.3 Identification of hazards 58](#_Toc157105898)

[4.4 Estimation of the clinical risks 59](#_Toc157105899)

[5.1 Risk evaluation 59](#_Toc157105900)

[6.1 Risk control 59](#_Toc157105901)

[6.2 Clinical risk benefit analysis 59](#_Toc157105902)

[Unacceptable risk management process 59](#_Toc157105903)

[Application of ALARP 60](#_Toc157105904)

[6.3 Implementation of clinical risk control measures 60](#_Toc157105905)

[7.1 Delivery, monitoring, and modification. 61](#_Toc157105906)

[7.2 Post deployment monitoring 61](#_Toc157105907)

[7.3 Modification 62](#_Toc157105908)

[Appendix: 62](#_Toc157105909)

[Demo video: 62](#_Toc157105910)

[Reference: 62](#_Toc157105911)

# 2.1 Risk Management process

We apply the DCB0160 risk management process shown here.

|  |
| --- |
| 1. Risk Analysis |
| * 1.1 Scope Definition (4.2) |
| * 1.2 Clinical Hazard Identification (4.3) |
| * 1.3 Clinical Risk Estimation (4.4) |
| 2. Risk Evaluation |
| * 2.1 Initial Clinical Risk Evaluation (5.1) |
| 3. Risk Control |
| * 3.1 Control Option Analysis (6.1) |
| * 3.2 Clinical Risk Benefit Analysis (6.2) |
| * 3.3 Control Measure Implementation (6.3) |
| * 3.4 Completeness Evaluation (6.4) |
| 4. Delivery and Monitoring |
| * 4.1 Delivery (7.1) |
| * 4.2 Post-deployment Monitoring (7.2) |
| * 4.3 Modification (7.3) |

# 2.2 Top Management Commitment

Our defined process for ensuring appropriate resources are assigned:

**1. Project Proposal**

* A partner or team member outlines the project's aim, timeline, and resource needs (e.g. staff time, IT support, funding) and the proposal is discussed at the partners' meeting.

**2. Resource Assessment**

* The partners review:
  + Staff availability (clinical/admin), Budget implications, Equipment or IT requirements
* Risks or constraints are identified (e.g. rota pressure, funding limits).

**3. Approval and Assignment**

* If agreed, resources are approved, and responsibilities are assigned to named individuals.

**4. Monitoring and Adjustment**

* Progress is reviewed at partner or team meetings.

# 2.3 Safety Officer

We have used an external clinical safety officer to ensure compliance with the DCB0160 standard.

**Clinical Safety officer:** Dr Nicola Turner, a GMC registered professional with formal training in clinical risk management certified via an NHS digital approved course.

# 2.4 Competencies of Personnel

Risk management competency is updated annually according to our internal practice training process. Our organisation use suitably qualified internal and external personnel to undertake risk management tasks and the maintenance of competencies. Internal records are held in our practice files, and external records of competence are found here (<https://www.clinitalk.co.uk/governance>)

# 2.5 Intelligent procurement

Clinitalk is not a health IT system. In the interest of best practice Clinitalk complies with the DCB0129 standard. No health IT system in the organisation or externally is reliant on Clinitalk or interoperates with it. Clinitalk has provided us with its compliance documentation, which can be found here (<https://www.clinitalk.co.uk/governance>)

The risks associated with Clinitalk are documented within the safety case report and hazard log.

# 2.6 Third party products assessment process

**Our DCB0160 Assessment Process**

| **Step** | **Action** | **Responsibility** |
| --- | --- | --- |
| 1️⃣ Identify Product | Confirm the product use i.e. is it for direct patient care requiring DCB0160 scope or other. | Practice Manager / IT Lead |
| 2️⃣ Request product Docs | Obtain the supplier’s Clinical Safety Case Report, Hazard Log, and compliance evidence | Practice Manager |
| 3️⃣ Appoint CSO | Nominate a trained Clinical Safety Officer (internal or external) | IT lead |
| 4️⃣ Conduct Local Risk Assessment | Review documentation and assess local risks | CSO |
| 5️⃣ Document Risk Controls | Identify and document any additional mitigations needed for safe use | CSO |
| 6️⃣ Create Clinical Safety Case Report | Summarise findings and confirm system is safe to deploy | CSO |
| 7️⃣ Maintain Safety Log | Record incidents, updates, and periodic reviews | IT lead |

We have confirmed Clinitalk is not a health IT system. Clinitalk has provided information about its compliance with the DCB0129 standard. We have completed a DCB0160 review as evidenced by this document.

# 2.7 Regular risk management process review

We review our risk process annually at our partners meetings.

Risks are brought to weekly management meetings as they are identified.

# 3.0 Project Safety Documentation and Repositories

Our risk documentation is versioned and previous versions stored so that changes can be tracked.

# 3.1 Risk Management File

This document forms our risk management file for the Clinitalk educational IT system. It will be maintained for the life of the system. All formal documents and evidence of compliance including decisions that influence risk management are recorded here.

**Our Safety Documentation Retention Process**

| **Step** | **Action** | **Responsibility** |
| --- | --- | --- |
| 1️⃣ Define Scope | Identify relevant documents (e.g. DCB0160, hazard logs, safety cases) | Practice Manager |
| 2️⃣ Assign Custodian | Nominate a named individual to oversee retention | IT lead |
| 3️⃣ Use Secure Storage | Store documents in a secure, access-controlled digital location (e.g. NHS OneDrive /SharePoint) | IT lead |
| 4️⃣ Apply Retention Schedule | Retain documentation for **minimum 8 years** after system decommission or last use, per [NHS Records Code of Practice](https://transform.england.nhs.uk/information-governance/guidance/records-management-code/) | IT lead |
| 5️⃣ Review Annually | Review storage and access annually to ensure integrity | IT lead |

# 3.2 Risk Management Plan

The scale of this plan is commensurate with the scale of clinical functionality of Clinitalk whilst addressing the clinical risk management activities specified in DCB0160.

## Definition of the Clinitalk IT system in its use context

Clinitalk is an educational tool designed to stimulate reflection and learning following a clinical encounter. The system provides structured, post-consultation feedback on communication and consultation skills, based on audio recordings of simulated or real consultations. Its function is solely educational, aimed at enhancing the quality of GP training through reflection.

The principal users are a general practice trainee and their clinical supervisor. The feedback provided by Clinitalk occurs at a time after the consultation has been completed and all clinical decisions have been made. Clinitalk does not provide clinical decision support and advises users that queries relating to clinical decision making should be discussed with their assigned clinical supervisor with consideration of current local and national guidelines.

As outlined in the terms and conditions the user agrees that Clinitalk content must not be used for purposes other than post consultation educational reflection.

Clinitalk does not:

- Provide information for the purpose of delivering health or social care;

- Support or manage the direct care of patients or service users;

- Interface with or form part of a clinical health IT system;

- Function as a medical device or accessory under the UK Medical Devices Regulations.

As such, Clinitalk is not used in the diagnosis, prevention, monitoring, treatment, or alleviation of disease.

## 3.2a Relevant procedures, policies and resources required to ensure effective and efficient risk management.

The procedures, policies and resources created by Clinitalk form the basis of the Clinitalk risk management plan and are found here: <https://www.clinitalk.co.uk/governance>

Our related policies (Information governance, data protection, IT security, significant event analysis and staff training) are in our practice files.

## 3.2b Project management processes

The project and quality management processes applied by Clinitalk are found here: <https://www.clinitalk.co.uk/governance>

## 3.2c Clinitalk system development lifecycle

The Clinitalk system lifecycle is documented in file 1028 here: <https://www.clinitalk.co.uk/governance>

**Current lifecycle stage:** operations and maintenance. i.e. the app is released and is being maintained to ensure ongoing functionality, security and performance.

## 3.2d Criteria used to estimate risk

Risk for each hazard is estimated based on the hazard severity, likelihood and resulting risk.

### Risk severity definitions

|  |  |  |
| --- | --- | --- |
| Severity | Definition | Example |
| Minor | An incident that has negligible impact on system functionality or operation. It may cause inconvenience or minor disruption but does not pose a significant risk to data safety, data security, or critical processes. | User interface glitch causing temporary display issues. |
| Significant | An incident with a noticeable impact on system functionality or performance, potentially affecting critical operations. While it may not pose an immediate threat to data safety, data security, or critical processes, it requires attention and timely resolution to prevent further complications. | Temporary loss of data connectivity or functionality with noticeable but minor impact.  Attack resulting in the release of a limited volume of encrypted data not readable by an attacker. |
| Considerable | An incident that causes a noticeable disruption to system functionality, potentially affecting efficiency or causing inconvenience. However, it does not pose an immediate threat to data safety, data security, or critical processes | Partial system outage affecting some functions with moderate user impact.  Data breach with release of encrypted data not readable by an attacker.  An unauthorised password breach allowing access to unencrypted data on a single account. |
| Major | An incident that causes a critical failure in the system, resulting in a severe disruption to operations. It poses a significant threat to data safety or data security, requiring urgent intervention and recovery efforts. | Loss of significant user data with potential data governance implications.  Data breach with release of a limited volume of unencrypted data.  Unauthorised password breaches allowing access to unencrypted data on more than one account. |
| Catastrophic | An incident that leads to a complete and irrecoverable failure of the system, causing catastrophic consequences. It poses an imminent threat to data safety or data security, requiring an emergency response. | Complete loss of user data with significant data governance implications.  Data breach with release of unencrypted data.  Widespread password breaches with access to unencrypted data. |

### Likelihood categories

A screenshot of a computer

Description automatically generated

### Risk matrix

A table of multicolored bars with text

Description automatically generated with medium confidence

### Risk Acceptability Definitions

A close-up of a hazard warning

Description automatically generated

## 3.2e Risk Activity Roles and Authority

Our organisation partners are responsible for managing our related policies (Information governance, Data Protection Impact Assessment, data protection, IT security, significant event analysis and staff training) which can be found in our practice files.

**Responsible personnel:** Partners, Practice manager and IT Clinical safety lead.

**Safety documentation approver:** IT Clinical safety lead

**Review period:** Annual (or earlier if significant change to the IT system occurs)

Clinitalk is responsible for maintaining its policies shown below and available at https://www.clinitalk.co.uk/governance

* Cyber essentials compliance summary
* Data Processing Agreement review and maintenance
* Information Security Management System review and maintenance
* Information Security policy review and maintenance
* Password protection policy review and maintenance
* Database credentials policy review and maintenance
* Cryptography control policy review and maintenance
* Disaster recovery plan review and maintenance
* Acceptable use policy review and maintenance
* Security Incident policy review and maintenance
* Access control policy review and maintenance
* Consent and storage policy review and maintenance
* User registration policy review and maintenance
* Personnel register review and maintenance
* Asset register & Audits review and maintenance
* GDPR compliance audit review and maintenance
* Change management policy review and maintenance.
* Annual training on data security policies review and maintenance
* Key dates review and maintenance
* Privacy notice review and maintenance
* Internal user registration policy review and maintenance
* Digital Technology Assessment Criteria review and maintenance
* Risk management file review and maintenance
* ICO self-assessment review and maintenance Penetration testing documentation
* Integrated Care Board Assurance Framework review and maintenance
* Data processing agreement customer review and maintenance
* Information classification policy review and maintenance
* Data security and protection toolkit review and maintenance

## 3.2f Additional resources required

We have used an external clinical safety officer to ensure compliance with the DCB0160 standard.

**Clinical Safety officer:** Dr Nicola Turner, a GMC registered professional with formal training in clinical risk management certified via an NHS digital approved course.

## 3.2i Monitoring and responding to safety incidents

Our organisation maintains a significant event log of all significant events where we document all reported items relating to safety concerns.

# 3.3 Hazard Log

## Key to the Clinitalk Hazard Log labels

|  |  |
| --- | --- |
| Columns | Description |
| Hazard number | A unique number for the hazard |
| Hazard name | A short descriptive name for the hazard |
| Hazard description | A brief description of the hazard |
| Potential Impact | Description of effect of hazard in the care setting and potential impact on the patient |
| Possible Causes | Possible cause(s) that may result in the hazard. These may be technical, human error, etc. Note: a hazard may have multiple causes |
| Existing Controls | Identification of existing controls or measures that are currently in place and will remain in place post implementation that provide mitigation against the hazard, i.e. used as part of initial Hazard Risk Assessment |
| Initial Hazard Risk Assessment | |
| Severity | The severity of the hazard as defined in [risk severity definitions](#_Clinitalk_risk_severity) |
| Likelihood | The likelihood of the hazard as defined in [Likelihood categories](#_Clinitalk_Likelihood_categories) |
| Risk Rating | The derived risk rating from the combination of likelihood and severity according to [risk matrix](#_Clinitalk_risk_matrix) |
| Additional Controls | |
| Design | Identification of design features or configurations implemented in the Health IT System to provide mitigation against the hazard. |
| Test | Identification of testing to be completed to provide mitigation against the hazard |
| Training | Identification of training to be implemented to provide mitigation against the hazard. |
| Business Process Change | Identification of any Business Process Changes implemented to mitigate against the hazard |
| Residual Hazard Risk Assessment | |
| Severity | The severity of the mitigated hazard as defined by Table 7 |
| Likelihood | The likelihood of the mitigated hazard as defined by Table 8 |
| Risk Rating | The derived mitigated risk rating from the combination of likelihood and severity according to Table 9 |
| Actions | |
| Summary | Summary of the action being taken regarding mitigation of the hazard or individual causes |
| Owner | The owner of the action |
| Hazard Status | The status of the hazard:  • 'Open' not all clinical risk management actions, owned by the Manufacturer, in respect of this hazard, have been completed.  • 'Transferred' all clinical risk management actions owned by the Manufacturer, in respect of this hazard, have been completed but not all actions, owned by the deploying Health Organisation, have been completed.  • 'Closed' all clinical risk management actions in respect of this hazard have been completed. |

## Safety incident / Significant event log

Our safety incident log is held in our practice significant event files.

## Hazard Log Table

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Hazard Name | Potential Impact | Possible Causes | Existing Controls | Initial Hazard Risk Assessment | | | Additional Controls | | | | Residual Hazard Risk Assessment | | | Actions | | Hazard Status |
| Severity | Likeli-hood | Risk Rating | Design | Test | Training | Business process change | Severity | Likeli-hood | Risk rating | Summary | Owner |
| 1 | Off Label use | **Context**  This hazard considers the scenario in which a user uses Clinitalk off label for clinical rather than educational purposes.  Clinitalk displays educational information drawn from national guidance, and RCGP publications.  If there was an error in the information displayed and the trainee used the information to inform a clinical decision the decision may be adversely impacted. | 1.User fails to understand that Clinitalk is strictly an educational tool for reflection and use in clinical decision making is off license and against terms and conditions for use. | Users are required to sign terms and conditions to ensure they have a clear understanding about the conditions for licensed use. There is clear warning against off license use within the software. | Minor | Low | 1 | Review of this hazard has led to the addition of a further control to prominently highlight licensed and unlicensed use on the pages that display educational information so that the user is in no doubt that information shown is not for use in clinical decision making.  [H1 Screenshot](#Hazard1Screenshot)  Further review **1/6/25** has led to an additional control to make notes text unelectable and uncopiable to prevent Clinitalk educational summaries being used in clinical notes. | Test display of new control message.  Message displays clearly.  After recording the educational notes are not selectable and not copiable. [Demo video](https://1drv.ms/v/c/3d337aebe0c12eef/EQaFHPktqQFEmHkM_LykCywB-dh-ZpSK-hY9rhkYV965Rw?e=G4Wr1Z) | Users receive instruction in the terms and conditions and in the pages displaying educational information. | N/A | Minor | Very Low | 1 – Acceptable, no further action required | No out-standing actions | N/A | Closed |
| 2. Information presented not accurately translated from national guidance. | Authoring process requires authors to faithfully represent guidance from respected national sources NICE, British National Formulary, RCGP publication, Respected journal. The policy mitigates against the risk of authoring error.  AI generated content is facilitated by retrieval augmented generation. Output compares transcript content to guideline content and comments on whether items ‘ appear consistent’ or ‘inconsistent’ with guidance. Output does not give opinion on the ‘correctness’ of the consultation and does not make recommendations. Direct links to guidance are provided. Feedback is in the form of questions to stimulate reflection. Generation accuracy has been evaluated (985 consultations 4/7/25) and is reviewed weekly to ensure high levels of accuracy. A warning that AI content may contain errors is prominently displayed | Minor | Low | 1 | Updated models and set up have improved accuracy when combining multiple tasks t achieve a rating colour of red/amber/green. | AI output evaluations.  Generation accuracy has been evaluated (985 consultations 4/7/25) and is reviewed weekly to ensure high levels of accuracy. | Content authors receive training on the faithful representation of guidance from national sources. All content is reviewed for accuracy.  Users are given guidance on the accuracy of AI generated content. | Update of content authoring process to improve documentation. | Minor | Very Low | 1 – Acceptable, no further action required | No out-standing actions | N/A | Closed |
| 2 | Server attack | Malicious attack on server results in a release of database stored encrypted data. | 1. Malicious attack by cyber criminals | Encryption – all data in transit to our servers and at rest in our servers is encrypted so that information captured by attackers in a data breach will be unreadable by an attacker.  Penetration testing – our software including code on the server has been audited by a certified third party to demonstrate it is robust.  Data minimization / storage limitation – data storage is limited to 21 days post recording to prevent unauthorised access or use of historical data.  Internal server request validation – requests to the server are internally validated enabling us to recognise and block external attack traffic.  Activity logs – We log all activity to recognise abnormal traffic so that we can respond.  Service agreements – our server providers have certified the physical security of their servers reassuring us of their security.  Clinitalk holds public and product liability insurance for up to £2 million | Significant | Very Low | 2 | Request message authentication to prevent corrupted versions of valid messages (as copied through https eavesdropping) being submitted in order to damage data and testing  Encryption testing – [screenshot](#Hazard2Screenshot) of encrypted data in database.  Penetration testing certificate  [Screenshot](#Hazard2Screenshot) of data deleted after 21 days. | We have tested our encryption, data minimisation, internal validation and activity logging controls and have external certified penetration testing. | Our staff are trained annually on our information security management policies and procedures. | N/A | Significant | Low | 2 – Acceptable and further risk reduction impractical | No out-standing actions | N/A | Closed |
| 3 | Password attack | A password attack results in unauthorised account access providing the attacker with access to unencrypted data. | 1. Weak password security. | Data validation – a password must meet the minimum standards set for complexity to be accepted. We use industry standard complexity requirements with a mix of cases, symbols, and letters to mitigate the risk of password breach.  Password creation guidance – we provide user guidance at the point of password creation to support creation of a unique password that is solely used for the Clinitalk account to mitigate against password breaches.  Multi factor authentication – We apply multi factor authentication as part of the sign in process. The user must enter a unique token generated at the time of sign in. The token is sent to the users registered email account.  Clinitalk holds public and product liability insurance for up to £2 million | Consider-able | Low | 2 | Display of user terms and warning messages. [Screenshots](#Hazard3Screenshot) | We have tested our encryption, data minimisation, internal validation and activity logging controls and have external certified penetration testing. | N/A | N/A | Consider-able | Low | 2 – Acceptable and further risk reduction impractical | No out-standing actions | N/A | Closed |
| 2. Inadequate brute force password protection | Password attempt time out – Multiple failed password attempts result in an exponentially escalating time out to protect against brute force attacks.  Multi factor authentication – We apply multi factor authentication as part of the sign in process. The user must enter a unique token generated at the time of sign in. The token is sent to the users registered email account.  Activity logs – We log all activity to recognize abnormal traffic so that we can respond.  Penetration testing – our software on the server has been audited by a certified third party to demonstrate it is robust.  Data minimization / storage limitation – data storage is limited to 21 days post recording to prevent unauthorised access or use of historical data.  Clinitalk holds public and product liability insurance for up to £2 million | Consider-able | Low | 2 | Activity log test – screenshot  Penetration testing certificate  Password time out testing – [screenshot](#Hazard3Screenshot)/video | We have tested our encryption, data minimisation, internal validation and activity logging controls and have external certified penetration testing. | N/A | N/A | Consider-able | Low | 2 – Acceptable and further risk reduction impractical | No out-standing actions | N/A | Closed |
| 4 | Sub-processor attack | Attack on the sub processor leads to a data breach of unencrypted data. | 1. Inadequate encryption | Our sub-processor is certified as compliant with health data processing regulations and encrypts data in transit and at rest.  Data minimisation – no data is stored on the sub-processor. Data is processed and immediately and irretrievably deleted.  Penetration testing – our sub processor is certified as meeting security requirements.  Data Processing Agreement – our data processing agreement is legally binding and meets all UK GDPR requirements on data security.  Clinitalk holds public and product liability insurance for up to £2 million | Consider-able | Low | 2 | Sub processor certification – [link](https://app.vanta.com/assemblyai/trust/7n80syl8zln1bn1qm3x8eg)  (SOC 2, GDPR, HIPAA) | We have reviewed sub processor testing - certifications and security documentation. | N/A | N/A | Consider-able | Low | 2 – Acceptable and further risk reduction impractical | No out-standing actions | N/A | Closed |
| 5 | Recording without consent | Doctor records a consultation without seeking explicit consent. | 1. Doctor errantly fails to ask a patient for consent to record the consultation. | Reminders to confirm patient consent prior to and during recording are displayed prominently next to the recording button.  Post recording the doctor is required to affirm that explicit consent has been given for the recording. If consent has not been given the recording is not processed and is deleted immediately and irretrievably. | Significant | Very low | 1 | Review of this control has determined adequacy of the current design. The current design does not allow the doctor to record with affirming explicit consent.  Display of user terms and warning messages – see [screenshots](#Hazard5Screenshot) | The alerts have been tested and display appropriately pre and post consultation recording. | No specific training required. | None | Significant | Very low | 1 – Acceptable, no further action required | None | N/A | Closed |
| 6 | Service down | Service failure prevents a user from recording a consultation or reviewing educational feedback causing temporary inconvenience to the user. | 1. Cyber-attack such as dedicated denial of service (DDOS) or other attack prevents user access to the service. | Server host cyber protection and internal monitoring- our hosting service monitors its servers to detect attack and provides mitigations. We also monitor our user logs to detect abnormal user activity.  Disaster recovery plan – we have a disaster recovery and major incident plan to restore service. | Minor | Low | 1 | Test of logging – see screenshots.  Test of disaster recovery plan – see test of backup and restore | None | None | None | Minor | Low | 1 – Acceptable, no further action required | None | N/A | Closed |
| Hardware failure | Server host hardware failure – our server hosts monitor their hardware and provide a service level agreement with a service uptime guarantee. | Minor | Low | 1 | Server – [service level agreements / security centre](https://www.microsoft.com/en-gb/trust-center/product-overview) | None | None | None | Minor | Low | 1 – Acceptable, no further action required | None | N/A | Closed |
| Software failure | Change management control – our change management control process means we release to a test environment before release to the production environment to protect against software failure.  Roll back – we can roll back to our previous state should we experience a software issue in the production environment to ensure service availability. | Minor | Low | 1 | [Roll back testing screenshot](#Hazard6Screenshot)  [Test environment screenshot.](#Hazard6Screenshot) | None | None | None | Minor | Low | 1 – Acceptable, no further action required | None | N/A | Closed |
| 7 | Inappro-priate sharing of recording | GDPR breach and a breach of the doctor’s license under their regulatory code | User shares the audio with another user account that is not the account of their trainer. | Account sharing controls – The user can only share their account with a trainer type account to prevent unauthorised sharing of recordings with other trainees.  User validation – we validate that the GMC number provided is genuine to help mitigate against the risk of fake accounts.  Terms and conditions – users are required to agree to responsible use detailing the recording and sharing of consultations to mitigate against unethical use. To the same purpose we remind Doctors of their duty to follow the strict ethical codes set by the GMC regulator.  Screen warning – At the point of sharing we provide a clear warning regarding unauthorised sharing of recordings to mitigate against unacceptable recording.  Data minimization / storage limitation – data storage is limited to 21 days post recording to prevent unauthorised access or use of historical data.  Clinitalk holds public and product liability insurance for up to £2 million | Considerable | Very Low | 2 | [Test of terms and conditions sharing warning messages.](#Hazard7Screenshot) | Display of user terms and warning messages. | None | None | Considerable | Very Low | 2 – Acceptable and further risk reduction impractical | None | N/A | Closed |

### Hazard Log Screenshots:

#### Hazard 1 Off Label Use Testing Screenshot: Testing warning messages regarding licensed use of Clinitalk next to educational information.

A screenshot of a medical survey

Description automatically generated A screenshot of a survey

AI-generated content may be incorrect. A close-up of a paper

AI-generated content may be incorrect.

#### Hazard 2 Server Attack Testing Screenshot: Test of Audio deletion after 21 days

A screenshot of a web page

Description automatically generated

[See also event logging shown in Hazard 6](#_Hazard_6_Service)

#### Hazard 3 Password Attack Testing Screenshot: Test of user warnings and time outs

A screenshot of a computer

Description automatically generated

[See also event logging shown in Hazard 6](#_Hazard_6_Service)

#### Terms and conditions page at registration

A screenshot of a computer

Description automatically generated

#### Hazard 5 Recording without consent: Testing warning messages

A screenshot of a phone

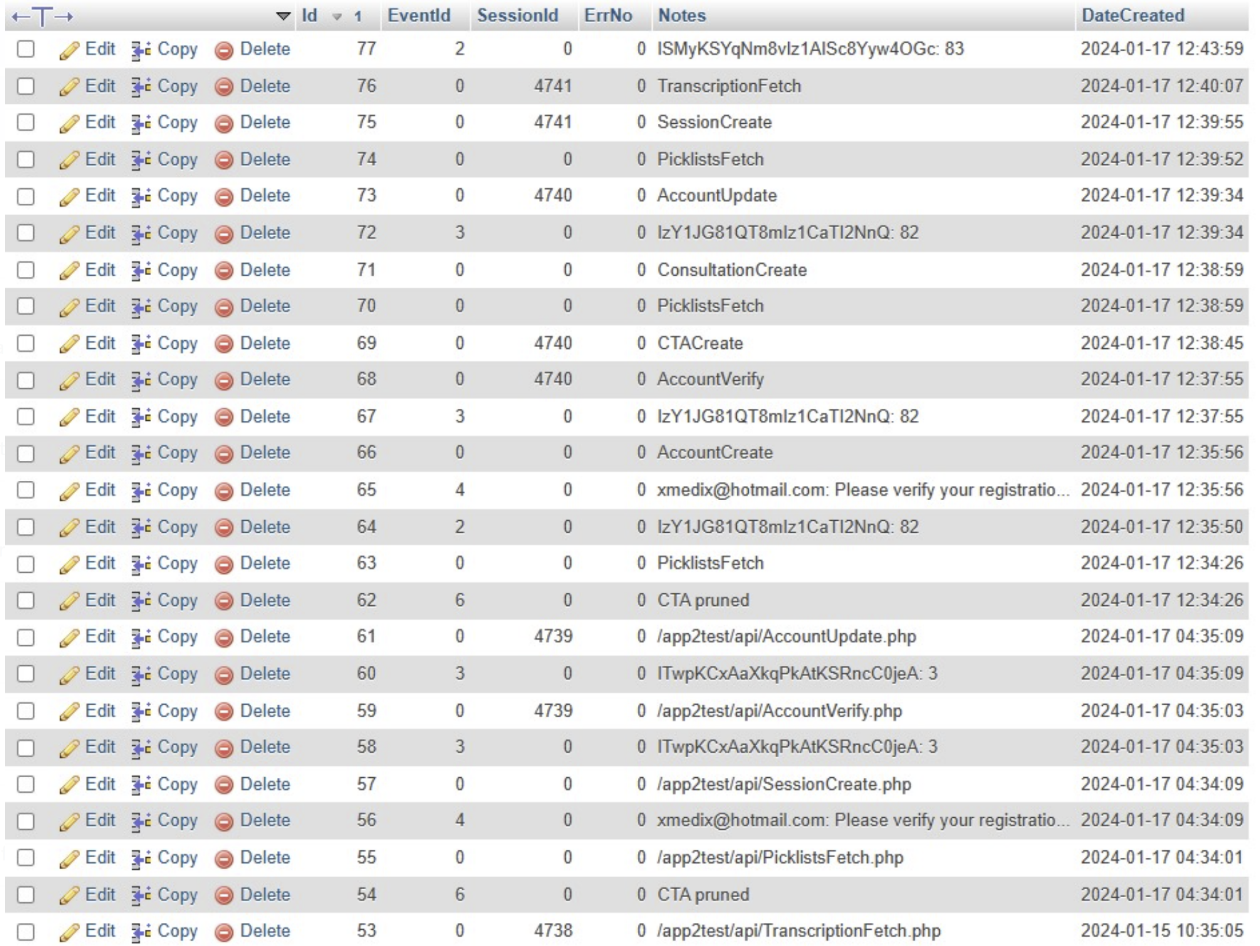
Description automatically generated A screenshot of a phone

Description automatically generated

See also our [terms and conditions page](#_Terms_and_conditions) which is shown at user registration. Agreement is a requirement for use of the service.

#### Hazard 6 Service Down Testing Screenshot: Testing logging and database backup and restore.

Screenshot showing the successful logging of user events.



Screenshot showing the successful logging of failed user log in attempts.

A screenshot of a computer

Description automatically generated

Screenshot showing a successful complete system restore test from backup for the purposes of disaster recovery using a separate server instance in a new geographical location. The address shows the new server location on the Microsoft azure platform.

A screenshot of a computer

Description automatically generated

###### Screenshot of restored data following a backup and restore test.

A screenshot of a medical test

Description automatically generated

###### Screenshot of Clinitalk running in a production test environment

A screenshot of a computer

Description automatically generated

#### Hazard 7 Inappropriate sharing of recording:

###### Terms and conditions warnings

A close-up of a box

Description automatically generated

See also our [terms and conditions page](#_Terms_and_conditions) which is shown at user registration. Agreement is a requirement for use of the service.

# 3.5 Safety Case Report

[Change Control](#ChangeControl)

## Introduction to the Safety Case Stages

### Stage 1 – Deployment

In stage 1 we trial the software. We review the hazards, considering any mitigations or amendments required.

### Stage 2 – Operations and maintenance

In stage 2 we plan the maintenance of the deployed software to ensure ongoing functionality, security, and performance. Stage 6 covers: monitoring of system performance, user support, routine updates, patches, and improvements. We review the hazards, considering any new hazards and any new mitigations or amendments required.

### Stage 3 – Change management.

In stage 3 we plan for the release of updates, enhancements, and bug fixes via a structured process. We review the hazards, considering any new hazards and any new mitigations or amendments required.

### Stage 4 – End of life (Retirement)

In stage 4 we plan decommissioning and communication of retirement at the end of the software’s meaningful life. We review the hazards, considering any new hazards and any new mitigations or amendments required.

### Stage 5 – Documentation and compliance

In stage5 we plan the documentation to ensure compliance with the regulations. We review the hazards, considering any new hazards and any new mitigations or amendments required.

### Stage 6 – Review and continuous improvement

In stage 6 we assess the effectiveness based on feedback and implement changes and lessons learned. We review the hazards, considering any new hazards and any new mitigations or amendments required.

## Product description – Safety Case

Clinitalk is an educational tool designed to stimulate reflection and learning following a clinical encounter. As outlined in the [terms and conditions](https://1drv.ms/w/s!Au8uweDrejM9itgVUFmCuu7Vi1zUZA?e=ltQZHM) the user agrees that Clinitalk content must not be used for purposes other than post consultation educational reflection. Usage outside of this scope is off license and unsupported.

A user accesses the Clinitalk URL using a web browser. New users create an account by registering using the provided link. Existing users log in with their credentials.

The user flows that describe the different user personas are found here: [User flows](https://1drv.ms/w/s!Au8uweDrejM9iuNLNbO20z-5yy6nhg?e=Il0A2p)

Users can record consultations via the ‘start a consultation’ button.

Feedback is provided to the user to stimulate reflection and learning following the clinical encounter.

The audio and consultation transcript can be reviewed by the user independently or with their trainer for up to 21 days following a clinical encounter. The analysis of performance and log of clinical encounters is retained and enables the trainee and trainer to review past performance and track progress.

# Safety Case Reports

### Report - stage 1 - Deployment

Purpose: The purpose of stage 1 is to consider the hazards associated with deployment.

##### System definition:

[View here](#_Definition_of_the)

##### Version: 1.2

##### Interoperability:

Clinitalk does not replace or interface with any existing systems. Clinitalk is not a health IT system.

##### Clinical risk management system:

As summarised in this document.

##### Key personnel:

Practice manager, Partners, IT lead, CSO (external).

We have used an external clinical safety officer to ensure compliance with the DCB0160 standard.

**Clinical Safety officer:** Dr Nicola Turner, a GMC registered professional with formal training in clinical risk management certified via an NHS digital approved course.

#### App Deployment process

None. Clinitalk is accessed via a secure web page. Approved browsers include Microsoft Edge, Google Chrome and Apple Safari. As per national cyber security guidance, to maintain a healthy device it is recommended that browser updates are installed as they become available.

#### System configuration

None. Clinitalk runs on any device with access to an approved web browser and has been tested on standard NHS issued desktop and laptop devices. There are no end user hardware, software, environment, or network configuration requirements.

#### System releases

* Release cycle
  + Monthly.
    - To provide a predictable rhythm for development and deployment releases are planned on a monthly release cycle.
* Release timing
  + Off Peak
    - Deployments are released in off peak hours (from 6pm to 8am) to minimise impact on users.
* Communication
  + Release information is provided to users via login screen messages, user email and via the Clinitalk website.

### Report - stage 1 - Risk evaluation

Hazard identification.

Hazard identification, risks identified at this stage:

1. [Off label use](#_Hazard_Log_Table)
2. [Server attack](#_Hazard_Log_Table)
3. [Password attack](#_Hazard_Log_Table)
4. [Sub processor attack](#_Hazard_Log_Table)
5. [Recording without consent](#_Hazard_Log_Table)
6. [Service down](#_Hazard_Log_Table)
7. [Inappropriate sharing of recording](#_Hazard_Log_Table)

The risks identified are described in the [hazard log](#_Hazard_Log_Table) alongside a description of the potential consequences, causes, existing mitigating controls, estimation of clinical risk and any outstanding actions. In the controls and additional controls sections of the hazard log the controls implemented are listed alongside a justification with links to test evidence and a residual risk evaluation. No outstanding test issues were found.

Summary safety statement from the Clinical Safety Officer: The risks at this stage carry a risk rating of between 1 and 2 and are assessed as acceptable to proceed to the next.

### Report - stage 1 - QA and Sign off:

Dr N.Turner. Clinical Safety Officer. 1/3/25

### Report - stage 2 - Maintenance

Purpose: The purpose of stage 2 is to maintain the deployed the solution to ensure ongoing functionality, security, and performance.

##### System definition:

[View here](#_Definition_of_the)

##### Version: 1.2

##### Interoperability:

Clinitalk does not replace or interface with any existing systems.

##### Clinical risk management system:

As summarised in this document.

##### Key personnel:

Practice manager, Partners, IT lead, CSO (external).

We have used an external clinical safety officer to ensure compliance with the DCB0160 standard.

**Clinical Safety officer:** Dr Nicola Turner, a GMC registered professional with formal training in clinical risk management certified via an NHS digital approved course.

#### Monitoring system functionality and performance

Clinitalk does not provide a health IT service and does not interoperate with our systems. As such it does not impact our function as a primary care provider. A failure of the Clinitalk service does not impact our organisations clinical function i.e. it is a non-critical system.

A summary of the testing, mitigations and evidence is provided in the hazard log, demonstrating that Clinitalk is a responsible supplier of educational software, compliant with external audit and assurance processes.

Clinitalk monitors system performance daily as part of their development operations task list. As a part of system monitoring, they log all user activity including user log in and failed user log in attempts and internal system errors and investigate anomalous activity.

In addition to the systematic monitoring, they monitor user queries relating to system performance.

Clinitalk has demonstrated a stable, secure and reliable service having been in operation for > 12 months delivering educational feedback on >8000 consultation recordings and passing multiple external audit processes from certified bodies.

##### Triggers for investigation

If our users (trainers or trainees) experience an error we require them to report the error to ourselves for information and to Clinitalk for them to investigate. We will record any significant issues in our significant event log.

### Report - stage 2 - Risk evaluation

Hazard identification, risks identified:

1. [Off label use](#_Hazard_Log_Table)
2. [Server attack](#_Hazard_Log_Table)
3. [Password attack](#_Hazard_Log_Table)
4. [Sub processor attack](#_Hazard_Log_Table)
5. [Recording without consent](#_Hazard_Log_Table)
6. [Service down](#_Hazard_Log_Table)
7. [Inappropriate sharing of recording](#_Hazard_Log_Table)

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the [hazard log](#_Hazard_Log_Table) alongside a description of the potential consequences, causes, existing mitigating controls, estimation of clinical risk and any outstanding actions. In the controls and additional controls sections of the hazard log the controls implemented are listed alongside a justification with links to test evidence and a residual risk evaluation. No outstanding test issues were found.

Summary safety statement from the Clinical Safety Officer: The risks at this stage carry a risk rating of between 1 and 2 and are assessed as acceptable to proceed to the next.

### Report - stage 2 - QA and Sign off:

Dr N.Turner. Clinical Safety Officer. 1/3/25

### Report - stage 3 - Change management

Purpose: The purpose of stage 3 is to plan for the controlled release of updates, enhancements, and bug fixes.

##### System definition:

[View here](#_Definition_of_the)

##### Version: 1.2

##### Interoperability:

Clinitalk does not replace or interface with any existing systems.

##### Clinical risk management system:

As summarised in this document.

##### Key personnel:

Practice manager, Partners, IT lead, CSO (external).

We have used an external clinical safety officer to ensure compliance with the DCB0160 standard.

**Clinical Safety officer:** Dr Nicola Turner, a GMC registered professional with formal training in clinical risk management certified via an NHS digital approved course.

#### Controlled release of updates, enhancements, and bug fixes

We will review the Clinitalk release update the information via: in app notifications, the Clinitalk website version history page.

### Report - stage 3 - Risk evaluation

Hazard identification, risks identified:

1. [Off label use](#_Hazard_Log_Table)
2. [Server attack](#_Hazard_Log_Table)
3. [Password attack](#_Hazard_Log_Table)
4. [Sub processor attack](#_Hazard_Log_Table)
5. [Recording without consent](#_Hazard_Log_Table)
6. [Service down](#_Hazard_Log_Table)
7. [Inappropriate sharing of recording](#_Hazard_Log_Table)

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the [hazard log](#_Hazard_Log_Table) alongside a description of the potential consequences, causes, existing mitigating controls, estimation of clinical risk and any outstanding actions. In the controls and additional controls sections of the hazard log the controls implemented are listed alongside a justification with links to test evidence and a residual risk evaluation. No outstanding test issues were found.

Summary safety statement from the Clinical Safety Officer: The risks at this stage carry a risk rating of between 1 and 2 and are assessed as acceptable to proceed to the next.

### Report - stage 3 - QA and Sign off:

Dr N.Turner. Clinical Safety Officer. 1/3/25

### Report - stage 4 - End of life

Purpose: The purpose of stage 4 is to plan for the applications decommissioning / end of life.

##### System definition:

[View here](#_Definition_of_the)

##### Version: 1.2

##### Interoperability:

Clinitalk does not replace or interface with any existing systems.

##### Clinical risk management system:

As summarised in this document.

##### Key personnel:

Practice manager, Partners, IT lead, CSO (external).

We have used an external clinical safety officer to ensure compliance with the DCB0160 standard.

**Clinical Safety officer:** Dr Nicola Turner, a GMC registered professional with formal training in clinical risk management certified via an NHS digital approved course.

#### End of life strategy

Strategy

##### 1. Notification and Communication:

- We will provide advance notice to users about the decision to retire the Clinitalk application.

- We will clearly communicate the reasons for discontinuation, whether it's due to technological advancements, changing business needs, or other factors and share information about the timeline for the shutdown and any alternatives or replacements that users can consider.

##### 2. User Data:

- All consultation data on Clinitalk is automatically deleted within 21 days of recording. Users may choose to maintain accounts to view historical educational feedback for the purpose of their learning log.

##### 3. Service Availability:

- We will specify the date on which we will retire the application.

##### 4. Support and Customer Service:

- We will handle user inquiries and issues via our IT lead.

##### 5. Documentation:

- We will update documentation to reflect the end-of-life status.

##### 6. Legal and Compliance Considerations:

- We will comply with any legal obligations, contracts, or agreements associated with Clinitalk’s use.

### Report - stage 4 - Risk evaluation

Hazard identification, risks identified:

1. [Off label use](#_Hazard_Log_Table)
2. [Server attack](#_Hazard_Log_Table)
3. [Password attack](#_Hazard_Log_Table)
4. [Sub processor attack](#_Hazard_Log_Table)
5. [Recording without consent](#_Hazard_Log_Table)
6. [Service down](#_Hazard_Log_Table)
7. [Inappropriate sharing of recording](#_Hazard_Log_Table)

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the [hazard log](#_Hazard_Log_Table) alongside a description of the potential consequences, causes, existing mitigating controls, estimation of clinical risk and any outstanding actions. In the controls and additional controls sections of the hazard log the controls implemented are listed alongside a justification with links to test evidence and a residual risk evaluation. No outstanding test issues were found.

Summary safety statement from the Clinical Safety Officer: The risks at this stage carry a risk rating of between 1 and 2 and are assessed as acceptable to proceed to the next.

### Report - stage 4 - QA and Sign off:

Dr N.Turner. Clinical Safety Officer. 1/3/25

### Report - stage 5 - Documentation and compliance

Purpose: The purpose of stage 5 is maintaining accurate documentation and ensuring compliance with relevant regulations.

##### System definition:

[View here](#_Definition_of_the)

##### Version: 1.2

##### Interoperability:

Clinitalk does not replace or interface with any existing systems.

##### Clinical risk management system:

As summarised in this document.

##### Key personnel:

Practice manager, Partners, IT lead, CSO (external).

We have used an external clinical safety officer to ensure compliance with the DCB0160 standard.

**Clinical Safety officer:** Dr Nicola Turner, a GMC registered professional with formal training in clinical risk management certified via an NHS digital approved course.

#### Audits

The audits, policies and documentation that document Clinitalk’s regulatory compliance are listed and accessible here <https://www.clinitalk.co.uk/governance>

Our documentation is included in this file and in the relevant documents in our practice files such as the significant event analysis log.

### Report - stage 5 - Risk evaluation

Hazard identification, risks identified:

1. [Off label use](#_Hazard_Log_Table)
2. [Server attack](#_Hazard_Log_Table)
3. [Password attack](#_Hazard_Log_Table)
4. [Sub processor attack](#_Hazard_Log_Table)
5. [Recording without consent](#_Hazard_Log_Table)
6. [Service down](#_Hazard_Log_Table)
7. [Inappropriate sharing of recording](#_Hazard_Log_Table)

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the [hazard log](#_Hazard_Log_Table) alongside a description of the potential consequences, causes, existing mitigating controls, estimation of clinical risk and any outstanding actions. In the controls and additional controls sections of the hazard log the controls implemented are listed alongside a justification with links to test evidence and a residual risk evaluation. No outstanding test issues were found.

Summary safety statement from the Clinical Safety Officer: The risks at this stage carry a risk rating of between 1 and 2 and are assessed as acceptable to proceed to the next.

### Report - stage 5 - QA and Sign off:

Dr N.Turner. Clinical Safety Officer. 1/3/25

### Report - stage 6 - Review and continuous improvement

Purpose: The purpose of stage 6 is to assess the effectiveness of the Clinitalk system and to make improvements.

System definition: [View here](#_Definition_of_the)

##### Version: 1.2

##### Interoperability:

Clinitalk does not replace or interface with any existing systems.

##### Clinical risk management system:

As summarised in this document.

##### Key personnel:

Practice manager, Partners, IT lead, CSO (external).

We have used an external clinical safety officer to ensure compliance with the DCB0160 standard.

**Clinical Safety officer:** Dr Nicola Turner, a GMC registered professional with formal training in clinical risk management certified via an NHS digital approved course.

#### Regular Reviews

Risk is reviewed at our regular partners meetings and annually. We review any reports of issues such as

* User feedback, positive and negative
* Reliability (down time)
* Performance (page load times, audio processing times)
* Security – review of any security incidents
* Costs – processing and maintenance costs
* Regulatory compliance – changes in the regulatory landscape

### Report - stage 6 - Risk evaluation

Hazard identification, risks identified:

1. [Off label use](#_Hazard_Log_Table)
2. [Server attack](#_Hazard_Log_Table)
3. [Password attack](#_Hazard_Log_Table)
4. [Sub processor attack](#_Hazard_Log_Table)
5. [Recording without consent](#_Hazard_Log_Table)
6. [Service down](#_Hazard_Log_Table)
7. [Inappropriate sharing of recording](#_Hazard_Log_Table)

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the [hazard log](#_Hazard_Log_Table) alongside a description of the potential consequences, causes, existing mitigating controls, estimation of clinical risk and any outstanding actions. In the controls and additional controls sections of the hazard log the controls implemented are listed alongside a justification with links to test evidence and a residual risk evaluation. No outstanding test issues were found.

Summary safety statement from the Clinical Safety Officer: The risks at this stage carry a risk rating of between 1 and 2 and are assessed as acceptable to proceed to the next.

### Report - stage 10 - QA and Sign off:

Dr N.Turner. Clinical Safety Officer. 1/3/25

# 4.1 Clinical risk analysis process

The clinical safety officer has ensured that the risk management activities outlined in the [clinical risk management plan](#_3.2_Risk_Management) have been implemented. Risk analysis has included the following:

Subject matter expert

Technical architect

Potential users

The clinical risk analysis has been deemed to be commensurate with the scale, complexity, and level of risk.

# 4.2 Scope Definition

## Scope and intended use:

Clinitalk is an educational tool designed to stimulate reflection and learning following a clinical encounter. As outlined in the terms and conditions the user agrees that Clinitalk content must not be used for purposes other than post consultation educational reflection. Usage outside of this scope is off license and unsupported.

Clinitalk does not provide clinical decision support and advises users that queries relating to clinical decision making should be discussed with their assigned clinical supervisor with consideration of current local and national guidelines.

## Human interface:

In defining the scope, we have considered the interaction of the user with the system and their behaviours. The associated hazards have been identified in the hazard log table and controls introduced to mitigate risk.

Infrastructure:

Clinitalk has a minimal infrastructure impact, as it runs as a web-based application and is therefore widely accessible across current devices.

## Operational environment

Clinitalk operates on a secure web page and requires a device with internet access and an approved browser which includes Microsoft Edge, Google Chrome and Apple Safari. As per national cyber security guidance, to maintain a healthy device it is recommended that browser updates are installed as they become available. Clinitalk is hosted in a secure cloud environment and accessed via standard networks and devices within the GP practice. Data is encrypted in transit and at rest and the detailed security and governance information is found here https://www.clinitalk.co.uk/governance

#### System configuration

None. Clinitalk has been tested on standard NHS issued desktop and laptop devices. There are no end user hardware, software, environment, or network configuration requirements.

# 4.3 Identification of hazards

Hazard Root cause analysis was facilitated using the fishbone technique to capture hazards across the end-to-end process. Hazards associated with the applications functionality and use of that functionality were considered. The Clinitalk system is a web based application and does not communicate with health IT messaging systems or health care system architectures and so no associated hazards exist in these areas. The identification of hazards workshop meeting minutes are documented here; [March 2023 workshop](https://1drv.ms/w/s!Au8uweDrejM9iuxNmYN7DoD3o2v9ZQ?e=tIgKKO) and [December 2023 workshop](https://1drv.ms/w/s!Au8uweDrejM9iuxPzS3BGQT3lNW8_Q?e=bGLM4U).

Hazards are documented in our [hazard log](#_3.3_Hazard_Log).

The hazards log considers known and foreseeable hazards in both normal and fault conditions.

# 4.4 Estimation of the clinical risks

For each identified hazard the severity, likelihood and resulting risk has been estimated using the [criteria specified](#_3.2d_Criteria_used) in the [risk management plan](#_3.2_Risk_Management). The estimation of risks is documented in the [hazard log table](#_Hazard_Log_Table).

The assessment of severity scale is documented [here](#_Clinitalk_risk_severity).

The assessment of likelihood scale is documented [here](#_Clinitalk_Likelihood_categories).

The two-dimensional risk matrix is documented [here](#_Clinitalk_risk_matrix).

# 5.1 Risk evaluation

For each individual hazard the acceptability of the initial risk has been evaluated and documented in the [hazard log table](#_Hazard_Log_Table). Risk ratings of 1 and 2 are deemed acceptable. Risk ratings of 3 or higher are deemed undesirable or unacceptable. Where the risk is acceptable the risk control requirements defined in 6.1 and 6.3 of this document do not apply to the hazard. The controls put in place prior to deployment are factored into the assessment. Where additional controls have been added the risk evaluation exercise post addition has been documented in the [hazard log table](#_Hazard_Log_Table).

The definitions of risk acceptability are documented [here](#_Clinitalk_Risk_Acceptability).

Clinitalk has been able to implement suitable control measures for each of the hazards identified.

# 6.1 Risk control

Risk control measures have been identified to mitigate the risks identified. The control measures and risk evaluation are documented in the [hazard log table](#_Hazard_Log_Table). As part of the evaluation, we considered whether the addition of control measures would introduce new hazards and whether the risks for previously identified hazards would be affected. The risk evaluations were reviewed and adjusted where required. Hazards were managed in accordance with the measure documented in sections 4.4 to 6.4 of this document. All risk has been evaluated against the risk criteria documented in the [risk management plan](#_3.2_Risk_Management). No unacceptable residual risks have been identified.

Risk reduction included but was not limited to considering changes in design, testing, administration, user training, and system warnings.

# 6.2 Clinical risk benefit analysis

Risk benefit is required for every hazard where the residual risk is deemed as unacceptable and further risk control is not practicable. As stated in 6.1 the current risk assessment state is that no unacceptable residual risks have been identified and therefore additional risk benefit analysis has not been performed.

## Unacceptable risk management process

Should an unacceptable residual risk be identified the Clinical safety officer supported by stakeholders shall determine whether the risk associated with the hazard is outweighed by the educational benefits of the system. In such circumstances the risk judgement will consider the technical, regulatory, economic, sociological, educational, clinical, and political context. If the analysis concludes that the risks outweigh the benefits the risk will remain unacceptable. Deployment shall only proceed once risk becomes acceptable which may be possible through the inclusion of additional control measures.

## Application of ALARP

The concept of ALARP (As Low As Reasonably Practicable) is accepted practice in risk benefit analysis and may be used to justify residual risk based on technical and economic practicability. The assessment is one of proportionality. Whilst it may be feasible to reduce the level of residual clinical risk through further mitigation or control the cost of doing so may be so great that it far outweighs the benefits to be gained in doing so. Conversely, there may be situations where for modest additional effort significant benefits in risk reduction could be realised. ALARP has been considered in the risk evaluation process.

A red and green triangle with white text

Description automatically generated

# 6.3 Implementation of clinical risk control measures

The clinical risk control measures documented in the [hazard log table](#_Hazard_Log_Table) have been implemented in the Clinitalk application. We have verified the clinical risk control measures and links to relevant evidence are documented in the hazard log table and the [safety case reports](#_Safety_Case_Reports). Other evidence such as logs, audits, and certification can be found in the [resources list](#_3.2a_Relevant_procedures,). The verification process considers both the implementation and effectiveness of the measures.

# 6.4 Completeness of clinical risk control

The clinical risks from all identified hazards have been considered and accepted. A summary detailing the risks and their evaluation is detailed in the [hazard log table](#_Hazard_Log_Table) and the accompanying the [safety case reports](#_Safety_Case_Reports).

# 7.1 Delivery, monitoring, and modification.

Top management have been adequately appraised of all work conducted and involved in each safety case report. To ensure that all requirements of this standard have been met, prior to delivery of the Clinitalk system a formal review has been completed and documented in each of the [safety case reports](#_Safety_Case_Reports). The reports and their associated evidence demonstrate that:

* the clinical risk management plan has been implemented and the outcomes recorded.
* the residual risk for each hazard is acceptable.
* appropriate methods are in place to obtain relevant post deployment information to feed back into the risk management system. In this respect the methods implemented are 1) data logging to monitor system usage and errors and 2) user feedback reports.

No outstanding defects remain unresolved, and no additional external controls are required from third parties.

# 7.2 Post deployment monitoring

Reported safety concerns are documented in our established significant event log which is maintained and regularly reviewed as part of our partner and team meetings.

The impact of safety concerns must be documented in the significant event log along with any such information on the on-going validity of the safety case. Where evidence is assessed to undermine the safety case corrective action must be taken in accordance with the [risk management plan](#_3.2_Risk_Management) and documented in the [safety case reports](#_Safety_Case_Reports).

Additionally, Clinitalk monitors the application performance and keeps logs of:

* All user activity including user log in and failed user log in attempts.
* Error reports

Users or concerned third parties may report concerns to Clinitalk via their contact email address which acts as our central point of contact.

# 7.3 Modification

The clinical risk management process documented here will be applied to any modifications or updates to the Clinitalk system. The application of the process will be commensurate with the scale and extend of the change and the introduction of new risks. A new safety case report will be issued to support any modifications to Clinitalk that change its risk.

An audit trail of all versions and patches released for deployment are held in the Clinitalk GIT repository and releases log within the dev ops log repository.

# Appendix:

## Demo video:

Demo video and end user information.

[www.clinitalk.co.uk](http://www.clinitalk.co.uk)