Clinitalk Risk Management File

Change control

Reviewer	Date	Comments	Version	Approval	Date
N.Boeckx (CEO) **P.Salmon (CTO)**	11/12/23	Initial risk management review	1.0	Dr P Salmon Dr N.Boeckx	23/12/23 22/12/23
N.Boeckx (CEO) **P.Salmon (CTO)**	1/4/2024	risk management review	1.0	Dr P Salmon Dr N.Boeckx	1/4/2024
N.Boeckx (CEO) **P.Salmon (CTO)** **N.Turner (CSO)**	1/4/2025	risk management review	1.0	Dr P Salmon Dr N.Boeckx	11/04/2025

Next review date: April 2026

Contents

2.1 Risk Management process

Clinitalk’s risk management process is outlined in figure 1 below.

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 Clinitalk Top Management Commitment

Clinitalk top management commits to the provision of sufficient resources and competent personnel in proportion to the scale of complexity with appropriate expertise in the development and assurance of the IT system.

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 team meetings.

The senior information risk officer for releases is Dr Peter Salmon.

The chief medical officer is Dr Nicholas Boeckx.

The clinical safety officer is Dr Nicola Turner.

2.3 Safety Officer

Note: 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.

Clinitalk is therefore an educational product and not a Health IT system as defined in *'DCB0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems'*

> DCB 0129 definition of a health IT system:
>
> *A Health IT System is defined as a product used to provide electronic information for health or social care purposes.*

As an educational tool Clinitalk is in scope for risk management but out of scope for clinical risk management.

Safety officer for the Clinitalk educational product: Dr Nicola Turner is a suitably qualified and experienced clinician holding a current registration with the General Medical Council

Dr Turner is supported by Dr Nicholas Boeckx who is a suitably qualified and experienced clinician holding a current registration with the General Medical Council knowledgeable who has had Clinical Safety Officer training in risk management and its application with experience authoring safety cases and hazard logs for certified medical devices i.e. AF advisor. He is committed to ensuring risk management process is followed.

The safety officer and senior information risk officer are responsible for reviewing and approving risk management documentation.

2.4 Competencies of Personnel

Clinitalk has sought knowledgeable, and experienced personnel and third parties appropriate to undertaking risk management tasks and the maintenance of competencies.

2.5 Third Party Products

Clinitalk uses a sub processor, and cloud services. Our asset register lists our software, hardware, and cloud assets. The assessment process and risks associated with third party products are documented within the safety case report and hazard log. Risks and their mitigations are also documented in our data processing impact assessment and our data processing agreement.

Sub processor Compliance checks:

We have checked our sub processor compliance against 10 key areas. Compliance is reviewed annually.

Security Feature	Status	Requirement and notes
Encryption in transit and at rest	✅	AES-256 at rest, TLS1.3 in transit (protects data from being read even if intercepted)
Role based access controls	✅	Sub processor applies strict organisational security by role
Active monitoring of service	✅	>99% uptime
External risk audits	✅	SOC2 standard
Penetration testing	✅	Annually tested against simulated cyber-attack
GDPR compliant	✅	Yes
PCI-DSS compliant	✅	Meets requirements for processing, storing, transmitting and accessing payment card information
No model training on data	✅	Yes
Data deletion post processing	✅	Yes
Data protection impact assessment	✅	In place

Storage: Note post processing in real time data is stored in encrypted format on Microsoft Azure servers in UK South.

2.6 Review of risk

Clinitalk assess risk on an annual basis and performs ad hoc risk reviews following actual or potential safety events. Risks are brought to weekly management meetings as they are identified, and a formal annual review is conducted of the whole management process.

3.0 Project Safety Documentation and Repositories

All Clinitalk risk documentation is versioned with change management controlled so that changes can be tracked.

3.1 Risk Management File

This document established at the start of the project forms the Risk Management File for the Clinitalk educational IT system. This file will be maintained for the life of the IT system. All formal documents and evidence of compliance is recorded in this file and any decisions made that influence the risk management activities are recorded in this file.

Step	Action	Responsibility
1️⃣ Define Scope	Identify relevant documents (e.g. DCB0129, hazard logs, safety cases)	Top management
2️⃣ Assign Custodian	Nominate a named individual to oversee retention	Top management
3️⃣ Use Secure Storage	Store documents in a secure, access-controlled digital location (e.g. NHS OneDrive /SharePoint)	SIRO
4️⃣ Apply Retention Schedule	Retain documentation for **minimum 8 years** after system decommission or last use, per NHS Records Code of Practice	SIRO

Step	Action	Responsibility
5️⃣ Review Annually	Review storage and access annually to ensure integrity	SIRO

3.2 Risk Management Plan

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 that form the basis of the Clinitalk risk management plan are listed here:

- Data Protection Impact Assessment
- Cyber essentials compliance summary
- Data Processing Agreement Assembly
- Information Security Management System
- Information Security policy
- Password protection policy
- Database credentials policy
- Cryptography control policy
- Disaster recovery plan
- Acceptable use policy
- Security Incident policy

- Access control policy
- Consent and storage policy
- User registration policy
- Personnel register [link not provided – contains personal data]
- Asset register & Audits
- Change management policy
- Annual training on data security policies
- Key dates
- Privacy notice
- Internal user registration policy
- Digital Technology Assessment Criteria
- Risk management file [this document]
- ICO self-assessment
- Penetration testing documentation
- Integrated Care Board Assurance Framework
- Data processing agreement customer
- Information classification policy
- Data security and protection toolkit
- Development operations log (Daily review of user logs for suspicious activity)
- Content authoring policy
- Customer contract and Data Sharing agreement

3.2b Project management processes

Project and quality management processes are described in our change management policy.

3.2c Clinitalk system development lifecycle

The Clinitalk system lifecycle involves several key stages, from conception to retirement. Each phase is crucial for ensuring the functionality, reliability, and security of the software. Below is an overview of the IT system lifecycle for the mentioned product:

Clinitalk Lifecycle and Risk Activities

1. Conception and Planning:

- Objective: Identify the need for a consultation recording software and define project scope and objectives.

- Activities:

  - Conduct market research to identify user needs and industry trends.

  - Define project goals, requirements, and constraints.

  - Create plan (see Innovate UK project plan), including timelines, resource allocation, and risk assessment.

⬇

2. Design:

- Objective: Develop a comprehensive design for the consultation recording software.

- Activities:

- Create detailed system specifications based on defined requirements.
- Design the software architecture, user interface, and database structure.
- Consider security measures and compliance with data protection regulations.

3. Development:

- Objective: Transform the design into a functional software system.
- Activities:
  - Write code according to coding standards and best practices.
  - Implement necessary features and functionalities.
  - Conduct regular code reviews and testing during the development process.

4. Testing:

- Objective: Ensure the software meets quality and performance standards.
- Activities:
  - Perform system testing, including regression testing.
  - Identify and fix bugs or issues through iterative testing.
  - Conduct user acceptance testing (UAT) with stakeholders.

5. Deployment:

- Objective: Release the software for production use.
- Activities:
  - Prepare for deployment, including data migration and system configuration.
  - Execute deployment during scheduled maintenance windows.
  - Monitor for any issues and implement a rollback plan if necessary.

6. Operations and Maintenance:

- Objective: Ensure the ongoing functionality, security, and performance of the software.
- Activities:
  - Provide user support and training.
  - Monitor system performance and address any issues promptly.
  - Implement routine updates, patches, and improvements.

7. Change Management:

- Objective: Manage changes to the software in a controlled and transparent manner.

- Activities:

  - Initiate change requests as needed for updates, enhancements, or bug fixes.

  - Review and approve changes through a Change Control Board.

  - Implement approved changes following a structured process.

⬇

8. End-of-Life (Retirement):

- Objective: Safely retire the software when it reaches the end of its useful life.

- Activities:

  - Develop a decommissioning plan.

  - Migrate data to a new system or archive as necessary.

  - Communicate the retirement to users and stakeholders.

⬇

9. Documentation and Compliance:

- Objective: Maintain accurate documentation and ensure compliance with relevant regulations.

- Activities:

  - Document all phases of the IT system lifecycle.

  - Conduct regular audits to ensure compliance with regulatory requirements.

⬇

10. Review and Continuous Improvement:

- Objective: Assess the effectiveness of the IT system lifecycle and make improvements.

- Activities:

  - Conduct regular reviews of the entire lifecycle.

  - Implement changes and improvements based on feedback and lessons learned.

3.2d Criteria used to estimate risk

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

Clinitalk 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	User interface glitch causing temporary display issues.

	significant risk to data safety, data security, or critical processes.	
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 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.

Clinitalk Likelihood categories

Likelihood Category	Interpretation
Very high	Certain or almost certain; highly likely to occur
High	Not certain but very possible; reasonably expected to occur in the majority of cases
Medium	Possible
Low	Could occur but in the great majority of occasions will not
Very low	Negligible or nearly negligible possibility of occurring

Clinitalk risk matrix

Likelihood	Very High	3	4	4	5	5
	High	2	3	3	4	5
	Medium	2	2	3	3	4
	Low	1	2	2	3	4
	Very Low	1	1	2	2	3
		Minor	Significant	Considerable	Major	Catastrophic
		Severity				

Clinitalk Risk Acceptability Definitions

5	Unacceptable level of risk Mandatory elimination of hazard or addition of control measure to reduce risk to an acceptable level
4	
3	Undesirable level of risk Attempts should be made to eliminate the hazard or implement control measures to reduce risk to an acceptable level. Shall only be acceptable when further risk reduction is impractical
2	Acceptable where cost of further reduction outweighs benefits gained or where further risk reduction is impractical
1	Acceptable, no further action required

3.2e Risk Activity Roles and Authority

The Safety Officer and Senior Information Risk Officer are jointly responsible for the creation, maintenance, and review of the following risk related activities:

- Data Protection Impact Assessment
- 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

Clinitalk risk management requires the following additional resources:

- Independent certified penetration testers
- Independent certified cyber security audit
- Integrated care board audit

3.2g Authority

The Safety Officer and Senior Information Risk Officer have the authority to jointly sign off risk activities and safety documentation.

3.2h Periodicity of review

Clinitalk assess risk on an annual basis and performs ad hoc risk reviews following actual or potential safety events. Risks are brought to weekly management meetings as they are identified, and a formal annual review is conducted of the whole management process to maintain an up to date and effective plan and to support a process of continual improvement.

3.2i Monitoring and responding to safety incidents

Our security incident policy outlines our procedures for monitoring and responding to safety incidents.

We keep logs of:

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

We monitor user logs daily as part of development operations task list which is monitored and updated by our senior information risk officer. Our logs are stored in the incident log.

All reported items relating to safety concerns must be stored and processed via the incident log.

3.2j The risk management plan review

Change control

Reviewer	Date	Comments	Version
N.Boeckx and P. Salmon and (Senior information risk officer)	12/12/23	Initial risk management plan review and sign off	1.0
N.Boeckx and P. Salmon and (Senior information risk officer)	1/4/24	Risk management plan review and sign off	1.1
N.Boeckx, P.Salmon,N.Turner	1/5/2025	Risk management plan review and sign off	1.2

Next review date: December 2024

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 Clinitalk risk severity definitions
Likelihood	The likelihood of the hazard as defined in Clinitalk Likelihood categories
Risk Rating	The derived risk rating from the combination of likelihood and severity according to Clinitalk risk matrix
Additional Controls	
Design	Identification of design features or configurations implemented in the Health IT System in order 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 log

The safety incident log is held here.

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.	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 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.	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 ‘	Minor	Low	1	N/A	N/A	Content authors receive training on the faithful representation of guidance from national sources. All content is reviewed for accuracy.	Update of content authoring process to improve documentation.	Minor	Very Low	1 – Acceptable, no further action required	No out-standing actions	N/A	Closed

				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) and is reviewed weekly to ensure high levels of accuracy. A warning that AI content may contain errors is prominently displayed													
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.	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 of encrypted data in database. Penetration testing certificate Screenshot 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 outstanding actions	N/A	Closed

				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.													
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.	Considerable	Low	2	Display of user terms and warning messages. Screenshots	We have tested our encryption, data minimisation, internal validation and activity logging controls and have external certified penetration testing.	N/A	N/A	Considerable	Low	2 – Acceptable and further risk reduction impractical	No outstanding 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	Considerable	Low	2	Activity log test – screenshot Penetration testing certificate Password time out testing – screenshot/video	We have tested our encryption, data minimisation, internal validation and activity logging controls and have external	N/A	N/A	Considerable	Low	2 – Acceptable and further risk reduction impractical	No outstanding actions	N/A	Closed

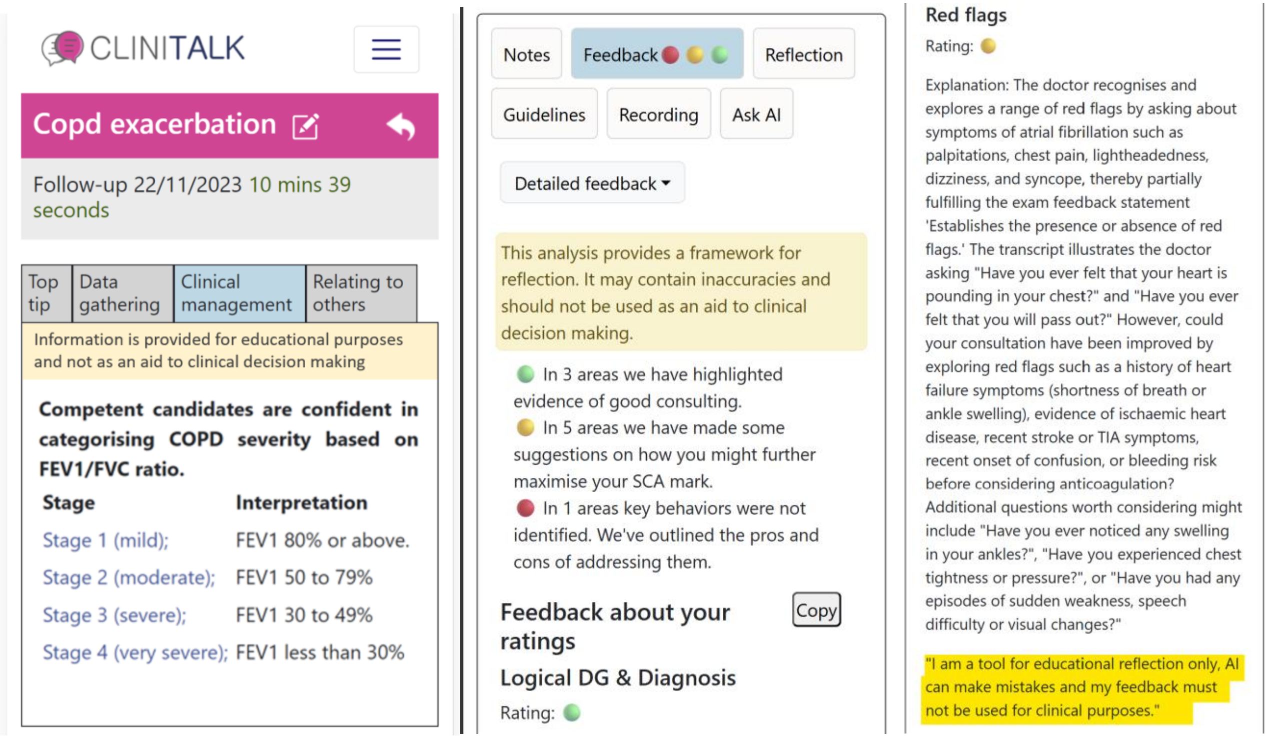
				apply multi factor authentication as part of the sign in process. The user must enter a unique token generated at the time of sign in. The token is sent to the users registered email account. Activity logs – We log all activity to recognize abnormal traffic so that we can respond. Penetration testing – 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.					certified penetration testing.								
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	Considerable	Low	2	Sub processor certification – (SOC 2, GDPR, HIPAA)	We have reviewed sub processor testing - certifications and security documentation.	N/A	N/A	Considerable	Low	2 – Acceptable and further risk reduction impractical	No outstanding actions	N/A	Closed

				requirements on data security.													
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	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	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.	Minor	Low	1	Roll back testing screenshot Test environment screenshot.	None	None	None	Minor	Low	1 – Acceptable, no further action required	None	N/A	Closed

				Roll back – we can roll back to our previous state should we experience a software issue in the production environment to ensure service availability.													
7	Inappropriate 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.	Considerable	Very Low	2	Test of terms and conditions sharing warning messages.	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.*



Copd exacerbation

Follow-up 22/11/2023 10 mins 39 seconds

Information is provided for educational purposes and not as an aid to clinical decision making

Competent candidates are confident in categorising COPD severity based on FEV1/FVC ratio.

Stage	Interpretation
Stage 1 (mild);	FEV1 80% or above.
Stage 2 (moderate);	FEV1 50 to 79%
Stage 3 (severe);	FEV1 30 to 49%
Stage 4 (very severe);	FEV1 less than 30%

This analysis provides a framework for reflection. It may contain inaccuracies and should not be used as an aid to clinical decision making.

- 🟢 In 3 areas we have highlighted evidence of good consulting.
- 🟡 In 5 areas we have made some suggestions on how you might further maximise your SCA mark.
- 🔴 In 1 areas key behaviors were not identified. We've outlined the pros and cons of addressing them.

Feedback about your ratings

Logical DG & Diagnosis

Rating: 🟢

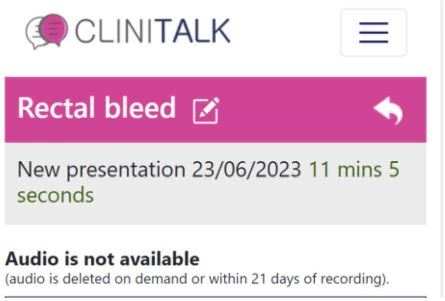
Red flags

Rating: 🟡

Explanation: The doctor recognises and explores a range of red flags by asking about symptoms of atrial fibrillation such as palpitations, chest pain, lightheadedness, dizziness, and syncope, thereby partially fulfilling the exam feedback statement 'Establishes the presence or absence of red flags.' The transcript illustrates the doctor asking "Have you ever felt that your heart is pounding in your chest?" and "Have you ever felt that you will pass out?" However, could your consultation have been improved by exploring red flags such as a history of heart failure symptoms (shortness of breath or ankle swelling), evidence of ischaemic heart disease, recent stroke or TIA symptoms, recent onset of confusion, or bleeding risk before considering anticoagulation? Additional questions worth considering might include "Have you ever noticed any swelling in your ankles?", "Have you experienced chest tightness or pressure?", or "Have you had any episodes of sudden weakness, speech difficulty or visual changes?"

"I am a tool for educational reflection only, AI can make mistakes and my feedback must not be used for clinical purposes."

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



Rectal bleed

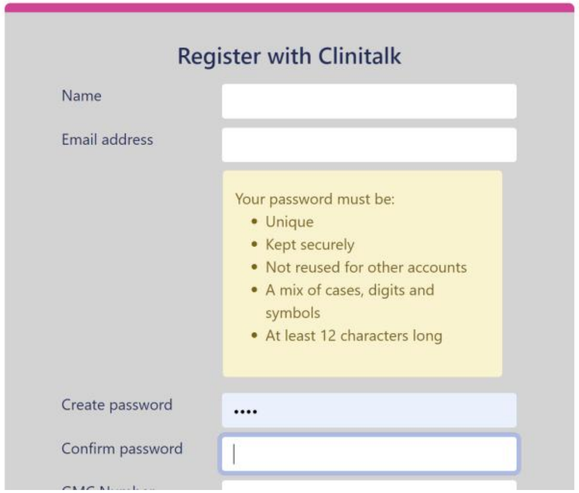
New presentation 23/06/2023 11 mins 5 seconds

Audio is not available

(audio is deleted on demand or within 21 days of recording).

See also event logging shown in Hazard 6

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



Register with Clinitalk

Name

Email address

Your password must be:

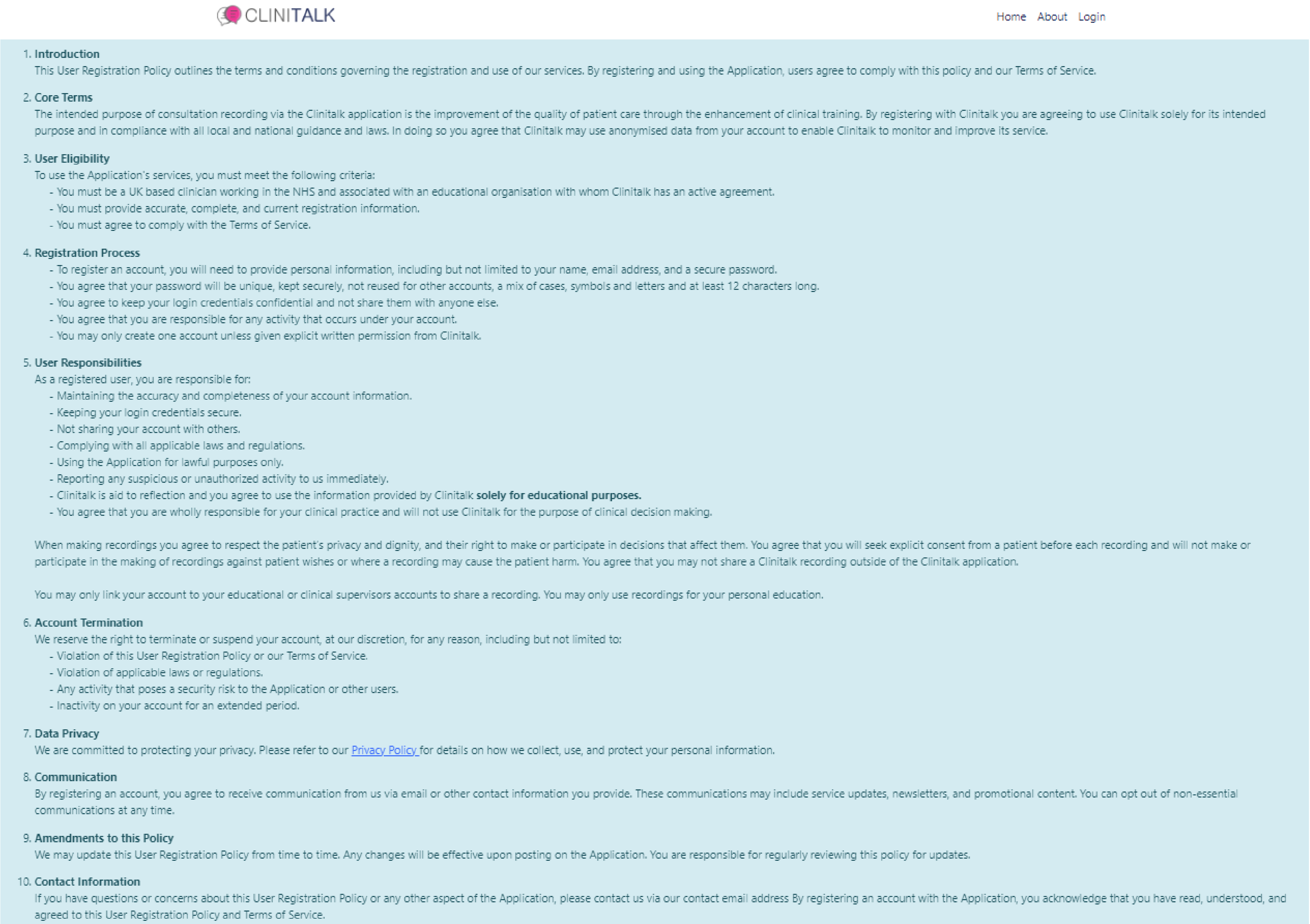
- Unique
- Kept securely
- Not reused for other accounts
- A mix of cases, digits and symbols
- At least 12 characters long

Create password ••••

Confirm password

See also event logging shown in Hazard 6

Terms and conditions page at registration



1. **Introduction**
   This User Registration Policy outlines the terms and conditions governing the registration and use of our services. By registering and using the Application, users agree to comply with this policy and our Terms of Service.

2. **Core Terms**
   The intended purpose of consultation recording via the Clinitalk application is the improvement of the quality of patient care through the enhancement of clinical training. By registering with Clinitalk you are agreeing to use Clinitalk solely for its intended purpose and in compliance with all local and national guidance and laws. In doing so you agree that Clinitalk may use anonymised data from your account to enable Clinitalk to monitor and improve its service.

3. **User Eligibility**
   To use the Application's services, you must meet the following criteria:
   - You must be a UK based clinician working in the NHS and associated with an educational organisation with whom Clinitalk has an active agreement.
   - You must provide accurate, complete, and current registration information.
   - You must agree to comply with the Terms of Service.

4. **Registration Process**
   - To register an account, you will need to provide personal information, including but not limited to your name, email address, and a secure password.
   - You agree that your password will be unique, kept securely, not reused for other accounts, a mix of cases, symbols and letters and at least 12 characters long.
   - You agree to keep your login credentials confidential and not share them with anyone else.
   - You agree that you are responsible for any activity that occurs under your account.
   - You may only create one account unless given explicit written permission from Clinitalk.

5. **User Responsibilities**
   As a registered user, you are responsible for:
   - Maintaining the accuracy and completeness of your account information.
   - Keeping your login credentials secure.
   - Not sharing your account with others.
   - Complying with all applicable laws and regulations.
   - Using the Application for lawful purposes only.
   - Reporting any suspicious or unauthorized activity to us immediately.
   - Clinitalk is aid to reflection and you agree to use the information provided by Clinitalk **solely for educational purposes.**
   - You agree that you are wholly responsible for your clinical practice and will not use Clinitalk for the purpose of clinical decision making.

   When making recordings you agree to respect the patient's privacy and dignity, and their right to make or participate in decisions that affect them. You agree that you will seek explicit consent from a patient before each recording and will not make or participate in the making of recordings against patient wishes or where a recording may cause the patient harm. You agree that you may not share a Clinitalk recording outside of the Clinitalk application.

   You may only link your account to your educational or clinical supervisors accounts to share a recording. You may only use recordings for your personal education.

6. **Account Termination**
   We reserve the right to terminate or suspend your account, at our discretion, for any reason, including but not limited to:
   - Violation of this User Registration Policy or our Terms of Service.
   - Violation of applicable laws or regulations.
   - Any activity that poses a security risk to the Application or other users.
   - Inactivity on your account for an extended period.

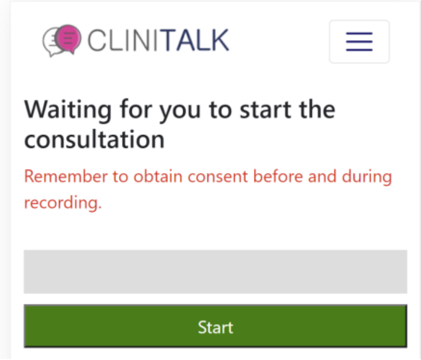
7. **Data Privacy**
   We are committed to protecting your privacy. Please refer to our Privacy Policy for details on how we collect, use, and protect your personal information.

8. **Communication**
   By registering an account, you agree to receive communication from us via email or other contact information you provide. These communications may include service updates, newsletters, and promotional content. You can opt out of non-essential communications at any time.

9. **Amendments to this Policy**
   We may update this User Registration Policy from time to time. Any changes will be effective upon posting on the Application. You are responsible for regularly reviewing this policy for updates.

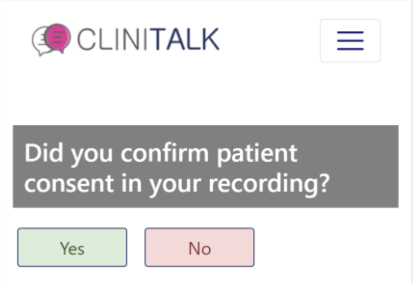
10. **Contact Information**
    If you have questions or concerns about this User Registration Policy or any other aspect of the Application, please contact us via our contact email address By registering an account with the Application, you acknowledge that you have read, understood, and agreed to this User Registration Policy and Terms of Service.

Hazard 5 Recording without consent: Testing warning messages



Waiting for you to start the consultation

Remember to obtain consent before and during recording.

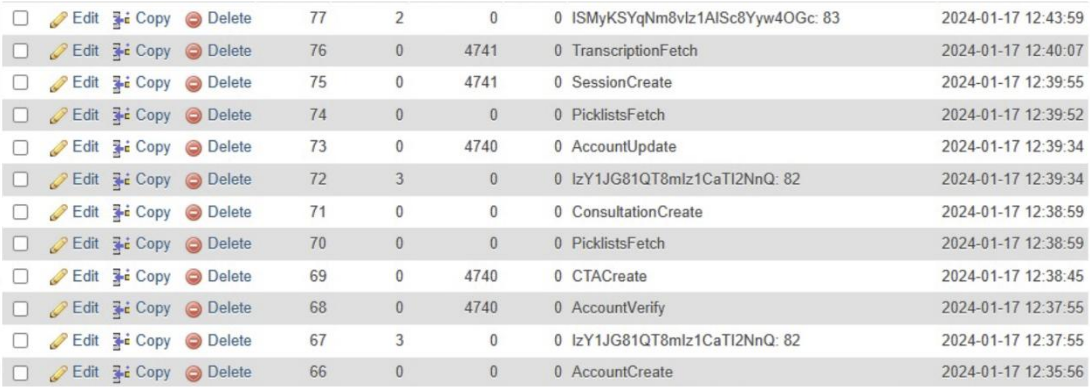


Did you confirm patient consent in your recording?

See also our terms and conditions page which is shown at user registration. Agreement is a requirement for use of the service.

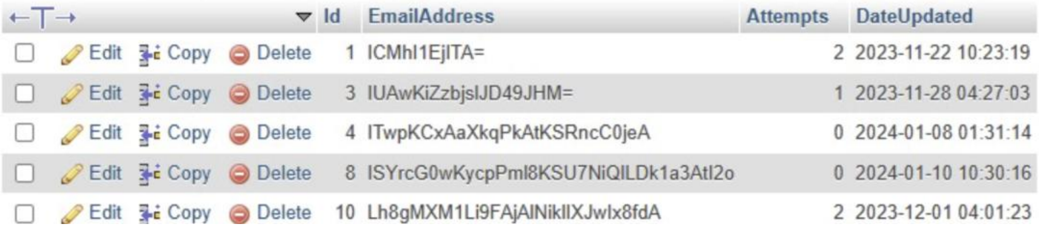
Hazard 6 Service Down Testing Screenshot: Testing logging and database backup and restore.

Screenshot showing the successful logging of user events.



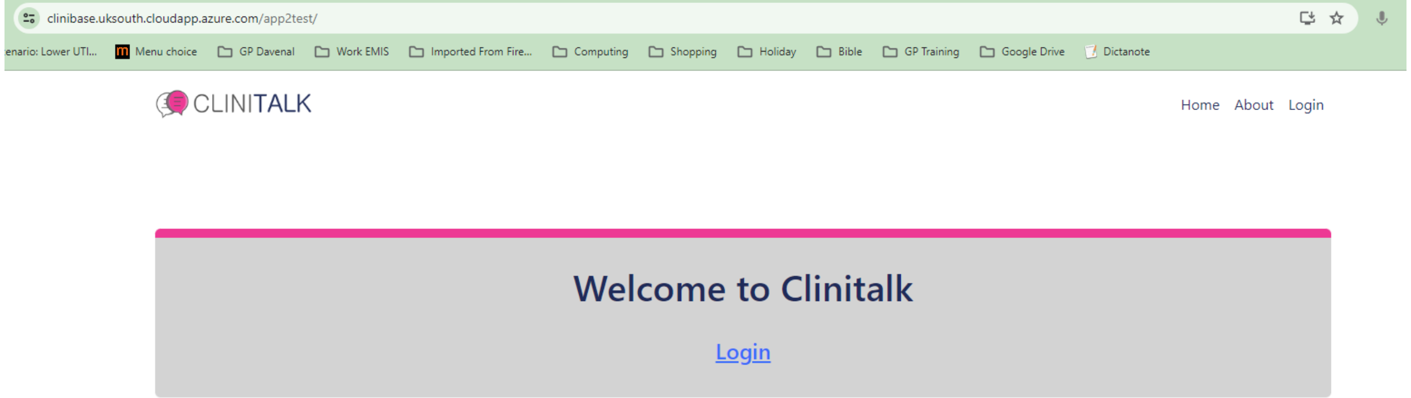
□	Edit	Copy	Delete	77	2	0	0	ISMyKSYqNm8vlz1AISc8Yyw4OGc: 83	2024-01-17 12:43:59
□	Edit	Copy	Delete	76	0	4741	0	TranscriptionFetch	2024-01-17 12:40:07
□	Edit	Copy	Delete	75	0	4741	0	SessionCreate	2024-01-17 12:39:55
□	Edit	Copy	Delete	74	0	0	0	PicklistsFetch	2024-01-17 12:39:52
□	Edit	Copy	Delete	73	0	4740	0	AccountUpdate	2024-01-17 12:39:34
□	Edit	Copy	Delete	72	3	0	0	IzY1JG81QT8mlz1CaTI2NnQ: 82	2024-01-17 12:39:34
□	Edit	Copy	Delete	71	0	0	0	ConsultationCreate	2024-01-17 12:38:59
□	Edit	Copy	Delete	70	0	0	0	PicklistsFetch	2024-01-17 12:38:59
□	Edit	Copy	Delete	69	0	4740	0	CTACreate	2024-01-17 12:38:45
□	Edit	Copy	Delete	68	0	4740	0	AccountVerify	2024-01-17 12:37:55
□	Edit	Copy	Delete	67	3	0	0	IzY1JG81QT8mlz1CaTI2NnQ: 82	2024-01-17 12:37:55
□	Edit	Copy	Delete	66	0	0	0	AccountCreate	2024-01-17 12:35:56

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



←T→			▼	Id	EmailAddress	Attempts	DateUpdated
□	Edit	Copy	Delete	1	ICMhl1EjITA=	2	2023-11-22 10:23:19
□	Edit	Copy	Delete	3	IUAwKiZzbjsIJD49JHM=	1	2023-11-28 04:27:03
□	Edit	Copy	Delete	4	ITwpKCxAaXkqPkAtKSRncC0jeA	0	2024-01-08 01:31:14
□	Edit	Copy	Delete	8	ISYrcG0wKycpPml8KSU7NiQILDk1a3AtI2o	0	2024-01-10 10:30:16
□	Edit	Copy	Delete	10	Lh8gMXM1Li9FAjAINikIIXJwIx8fdA	2	2023-12-01 04:01:23

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.

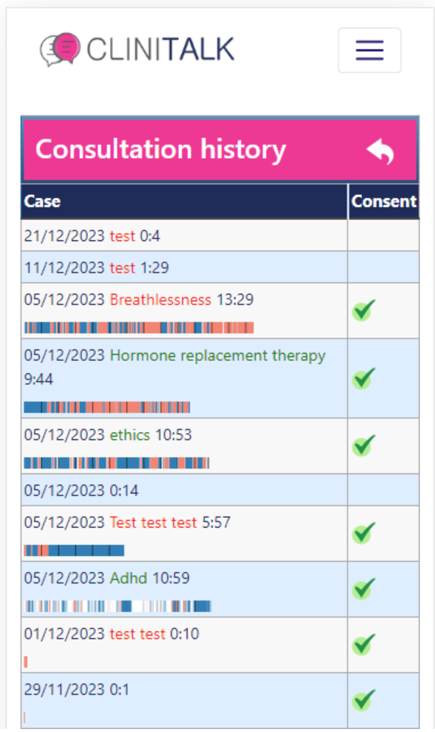


clinibase.uksouth.cloudapp.azure.com/app2test/

Welcome to Clinitalk

Login

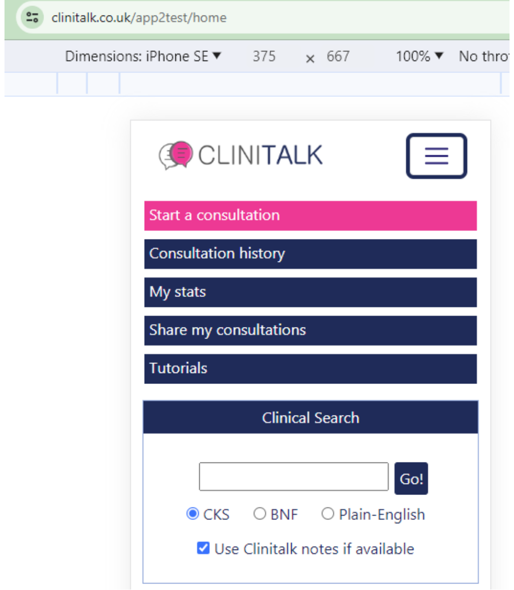
Screenshot of restored data following a backup and restore test.



Consultation history

Case	Consent
21/12/2023 test 0:4	
11/12/2023 test 1:29	
05/12/2023 Breathlessness 13:29	✓
05/12/2023 Hormone replacement therapy 9:44	✓
05/12/2023 ethics 10:53	✓
05/12/2023 0:14	
05/12/2023 Test test test 5:57	✓
05/12/2023 Adhd 10:59	✓
01/12/2023 test test 0:10	✓
29/11/2023 0:1	✓

Screenshot of Clinitalk running in our production test environment



clinitalk.co.uk/app2test/home

Dimensions: iPhone SE ▾ 375 × 667 100% ▾ No thro

CLINITALK

Start a consultation

Consultation history

My stats

Share my consultations

Tutorials

Clinical Search

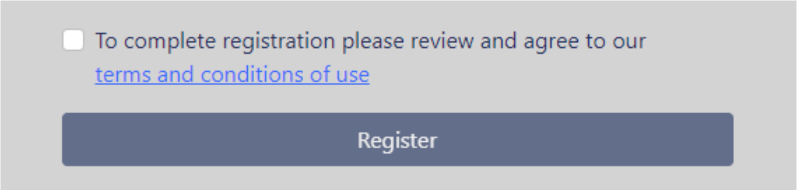
Go!

● CKS ○ BNF ○ Plain-English

☑ Use Clinitalk notes if available

Hazard 7 Inappropriate sharing of recording:

Terms and conditions warnings



□ To complete registration please review and agree to our terms and conditions of use

Register

See also our terms and conditions page which is shown at user registration. Agreement is a requirement for use of the service.

3.4 Safety Case Report

Change Control

Introduction to the Safety Case Stages

Stage 1 – Conception and planning

In stage 1 we investigate the market to identify user needs and industry trends relating to the market for an educational tool for GP training. The market investigation will be specific to the stimulation of reflection and learning following a clinical encounter. We consider safety risks and mitigations.

Stage 2 – Design

In stage 2 we design the educational tool to address the needs identified in Stage 1. The design contains the software architecture, user interface and database structure and considers security measures, and compliance with data protection regulations. We review the hazards, considering any new hazards and any new mitigations or amendments required.

Stage 3 – Development

In stage 3 we develop the educational tool to the design laid down in Stage 2. The development transforms the design into functional software that implements the necessary features and functionalities. The code is to be reviewed and tested during the stage 3 process. We review the hazards, considering any new hazards and any new mitigations or amendments required.

Stage 4 – Testing

In stage 4 we test the educational tool developed in stage using regression and system testing. We identify and fix bugs using an iterative testing approach and conduct user acceptance tests with stakeholders. We review the hazards, considering any new hazards and any new mitigations or amendments required.

Stage 5 – Deployment

In stage 5 we release the software tested in stage 4. The deployment planning includes roll back plans and plans for system configuration and deployment scheduling. We review the hazards, considering any new hazards and any new mitigations or amendments required.

Stage 6 – Operations and maintenance

In stage 6 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 7 – Change management.

In stage 7 we plan for the controlled 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 8 – End of life (Retirement)

In stage 8 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 9 – Documentation and compliance

In stage 9 we plan the documentation to ensure compliance with the regulations including audits. We review the hazards, considering any new hazards and any new mitigations or amendments required.

Stage 10 – Review and continuous improvement

In stage 10 we assess the effectiveness based on reviews of the lifecycle and 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 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

Users of the type 'GP trainee' can record consultations via the 'start a consultation' button.

Feedback is provided to the user to stimulate reflection and learning following the clinical encounter (typically within 60 seconds of completing 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.

3.5 Safety Case Reports

Report- stage 1- Conception and planning:

Stage 1 – Purpose (Conception and planning)

Stage 1: To conduct market investigation to identify user needs and industry trends.

System definition:

View here

Version: 1.0

Interoperability:

Clinitalk does not replace or interface with any existing systems.

Clinical risk management system:

Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

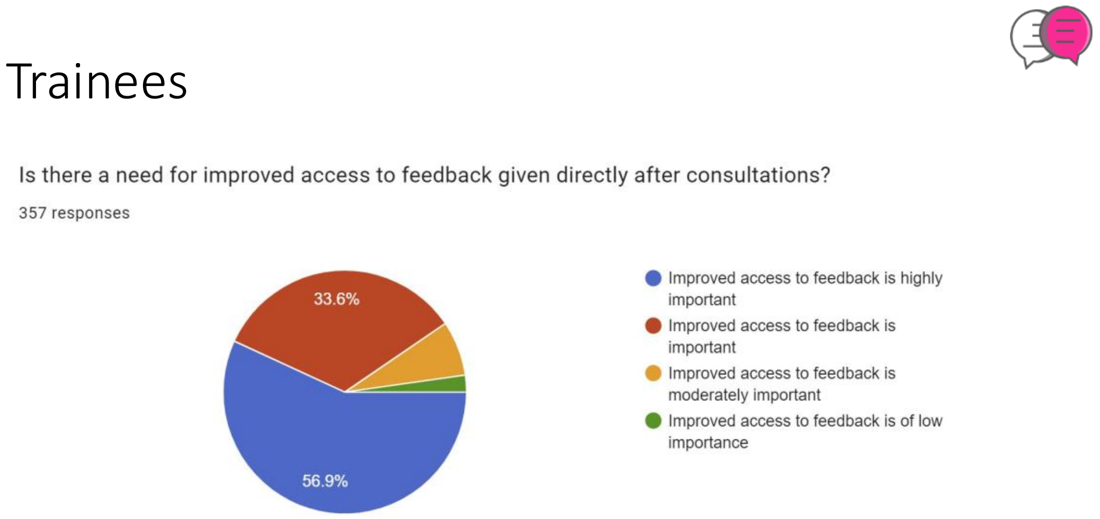
Key personnel:

Safety officer, Competencies

Stage 1 - Literature review:

- Huge GP shortfall (10 000) predicted to be 15K shortfall by 2036 *(source – NHS workforce planning papers).* There is a pressing need to recruit more qualified GPs.
- Lack of training resource is a barrier to the rate of trainee development and throughput *(source – differential attainment reports and workforce planning papers)*
- There is a differential attainment in sizeable trainee subgroups *(source – RCGP Chief examiner reports).*
- System wide lack of trainers, training time and training places. The pool of trainers is limited, and trainer resource is costly and difficult to scale. *(source – NHS workforce planning papers)*
- Investment in healthcare training is a government priority- *2023 NHS 15 YEAR WORKFORCE PLAN* .. improving quality and training numbers* Aiming for an additional 1000 GP training places by 2027 to 6000 by 2031. *(source – NHS workforce planning papers)*

Stage 1 - Survey results



Trainees

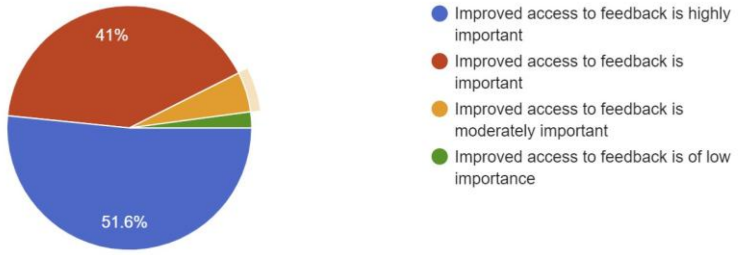
Is there a need for improved access to feedback given directly after consultations?

357 responses

Trainers

Is there a need for improved resource to enable post consultation feedback to be given to a greater proportion of trainee consultations?

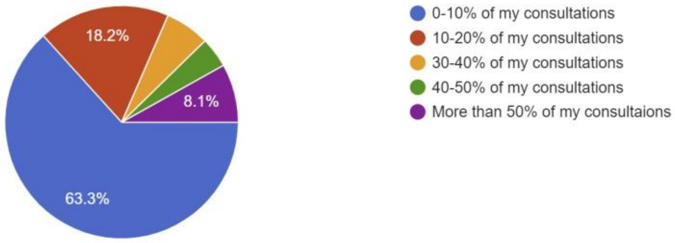
283 responses



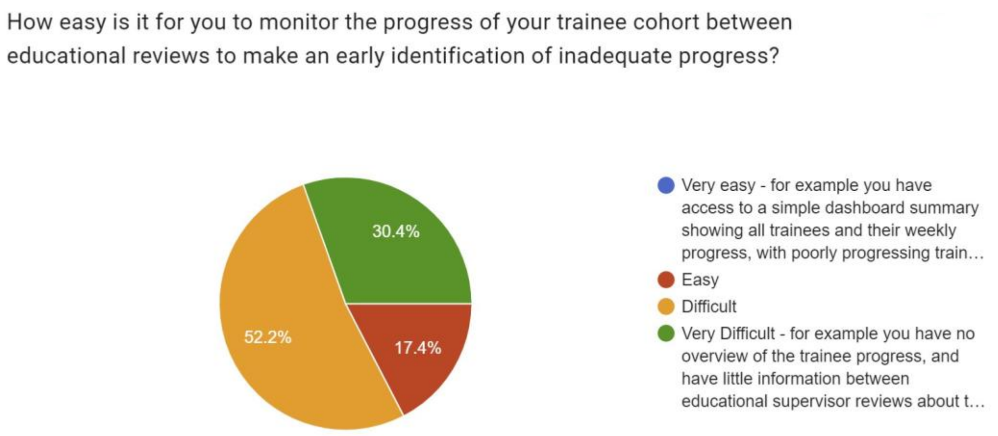
Trainees

On average in a week, what proportion of your consultations are observed by a trainer who gives you feedback about your consulting style and management?

357 responses



Training program directors


How easy is it for you to monitor the progress of your trainee cohort between educational reviews to make an early identification of inadequate progress?

Stage 1 - Market investigation conclusions

- Trainees, trainers, and training program directors and government recognise the pressing need to address demand.
  - 90% of trainees surveyed (373) recognise post consultation feedback as critical for their development yet 90% report that the majority (80-90%) of their consultations receive no feedback.
  - 92% of trainers surveyed (296) recognise post consultation feedback as critical for trainee development and conclude that additional resources are needed.
  - 85% of training program directors surveyed (24) report it is difficult to monitor trainees to enable the early identification of failing trainees.
    (source – Clinitalk trainee, trainer, and training program director surveys).
- Significant unmet training demand, specifically time for trainee mentoring *(source – Clinitalk trainee, trainer, and training program director surveys).*
- 80-90% of GP trainee consultations are unobserved, and by making those observed and included as part of workplace based assessment, the trainee has greater drive to implement learning in their daily consultations. The effect can be bolstered through rapid feedback loops post consultation and cumulative dashboards of performance.
- Failure to start preparation early, and a reliance on last minute cramming is a recognised contributing factor towards trainee exam failure, a behaviour challenged by the knowledge of being observed daily. *(source – RCGP Chief examiner reports).*

To summarise, there is a role for a digital solution where none currently exists to address the pressing need for more trainee mentoring in response to the lack of human resource and the costs of scaling. A digital solution has the potential to be hugely beneficial in terms of its ability to scale and it's relative cost.

Such a solution could help trainees to develop their clinical knowledge and consultation skills and in doing so collect data that enables training programs to remotely monitor progress of trainees and thereby identify and address training issues early.

The application could support GP training by encouraging the kind of personal reflection a GP trainer might stimulate were they able to sit in on every consultation. Using an innovative audio analysis and insights engine it could present relevant, tailored feedback after each consultation alongside statistical analysis. Feedback may be shared with the trainer as input into joint reviews and to allow remote monitoring.

Regular use by trainees will build an objective picture of their training progress which can be used to populate live dashboards that inform the training program of the performance of their trainees. Struggling trainees can be identified in a way that is not currently possible, and the results of interventions monitored (some of which may be delivered through the Clinitalk application). The concept is novel, no similar applications exist, and such dashboards would provide direct benefits to the training program directors who work on behalf of Health Education England which holds the purse strings.

Stage 1 - Goals

1. Create an easy to use solution that meets the identified needs of trainees, trainers, and training program directors.

Stage 1 – Requirements

Policies built around the requirements can be found here.

1. Information security control
2. Disaster recovery
3. Access control
4. Asset registration and audit
5. Change management
6. Staff training
7. GDPR compliance
8. Security testing and certification
9. Data impact assessment
10. Cryptography control
11. Privacy notification
12. Content authoring control

Stage 1 - Project Plan

Project plan document

Report - stage 1- Risk evaluation

Hazard identification, risks identified at this stage:

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

The risks identified are described in the hazard log 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:

This document has been reviewed and signed off by: Dr N.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) April Date: April 2023

Report - stage 2- Design

Stage 2 – Purpose (Design)

To design the educational tool to address the needs identified in Stage 1 including:

- Software architecture
- User interface
- Database structure
- Security measures

System definition:

View here

Version: 1.0

Interoperability:

Clinitalk does not replace or interface with any existing systems.

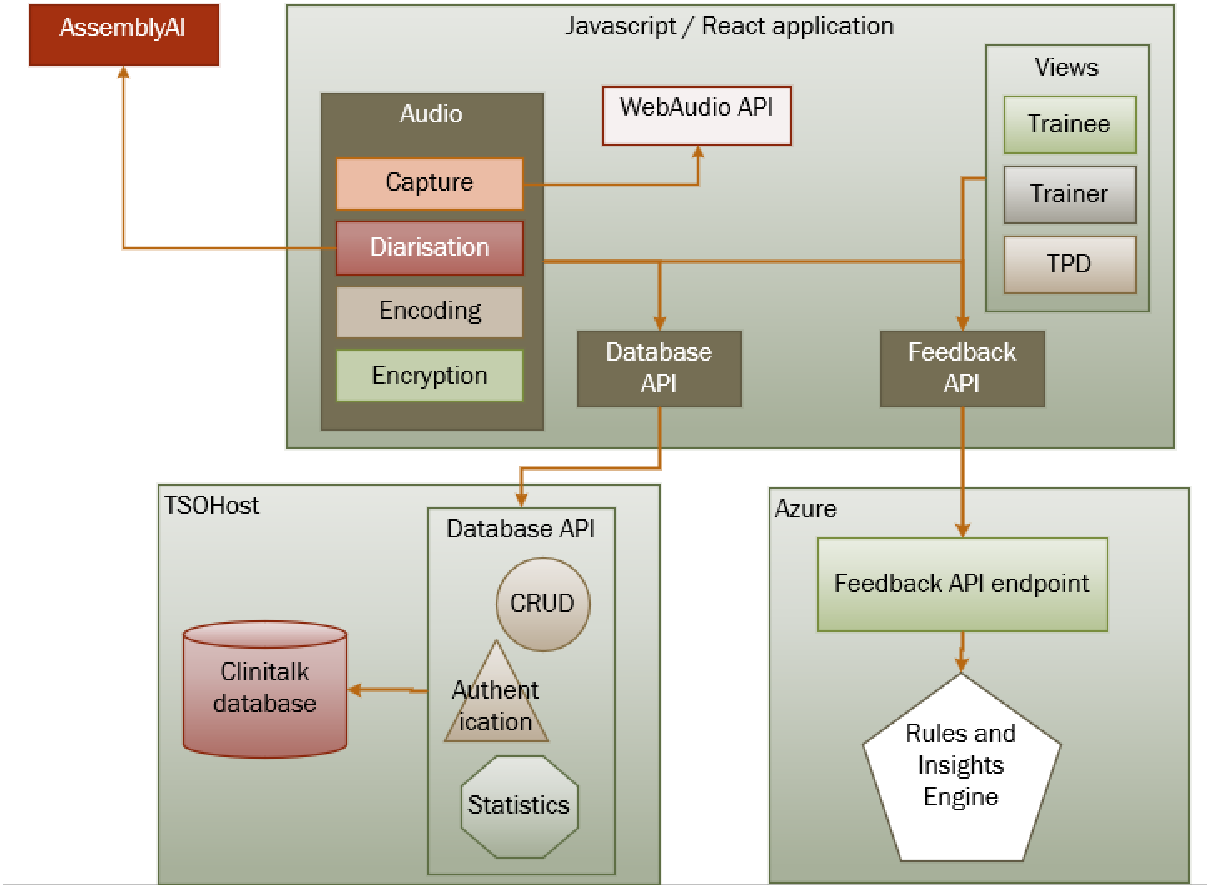
Clinical risk management system:

Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

Key personnel:

Safety officer, Competencies

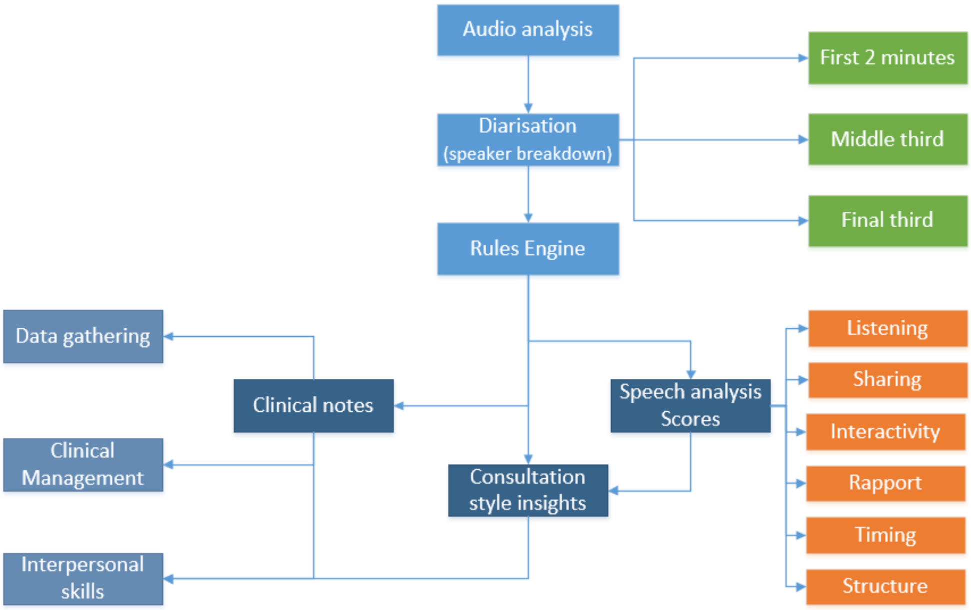
Stage 2 – Software architecture



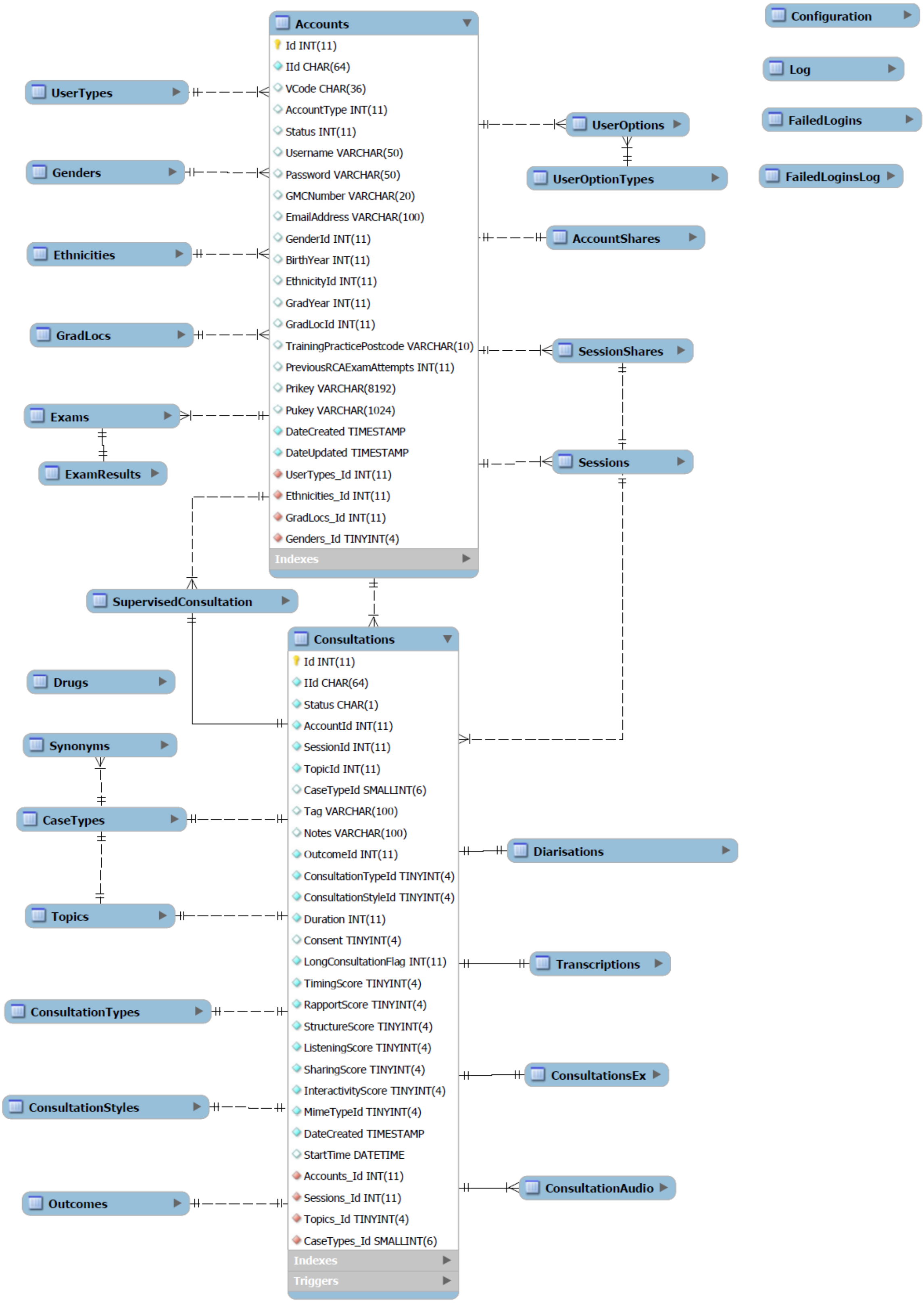
Stage 2 – User interface

The user interface design development can be found here.

Stage 2 – Feedback creation process



Stage 2 – Database structure



Stage 2 – Security measures

Our security design measures have been recorded in the following documents.

- Cyber essentials compliance summary
- Information Security Management System
- Password protection policy
- Database credentials policy
- Cryptography control policy
- Security Incident policy
- Access control policy
- Consent and storage policy
- User registration policy
- Asset register & Audits
- Change management policy
- Annual training on data security policies
- Internal user registration policy
- Digital Technology Assessment Criteria
- Penetration testing documentation
- Integrated Care Board Assurance Framework
- Data processing agreement customer
- Information classification policy
- Data security and protection toolkit
- Development operations log (Daily review of user logs for suspicious activity)

Stage 2 – Data protection regulation compliance

Our data protection regulation compliance has been recorded in the following documents.

- Data Protection Impact Assessment
- Data Processing Agreement Assembly
- Information Security policy
- Acceptable use policy
- GDPR compliance audit
- Privacy notice
- ICO self-assessment

Report - stage 2- Risk evaluation

Hazard identification, risks identified at stage 2:

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

CLINITALK takes the protection of data seriously will adhere to GDPR, GMC and RCGP standards and guidance. We take the protection of consultation data seriously. All consultations will be securely stored to prevent against unauthorised access or interception. We use industry standard AES256 encryption, one of the strongest security technologies available. Consultation data will only be de-encrypted by the user and their trainer if they have linked to their trainer's account . CLINITALK itself will not be able to access recordings. All data will be encrypted in transit and at rest and tested by an external licensed third party to assure the security.

Focus groups were used to inform user interface design. A record of the user design development can be found here: Clinitalk user experience design record.

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the hazard log 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:

Sign off by: Dr N.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) April Date: May 2023

Report - stage 3 - Development

System definition:

View here

Version: 1.0

Interoperability:

Clinitalk does not replace or interface with any existing systems.

Clinical risk management system:

Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

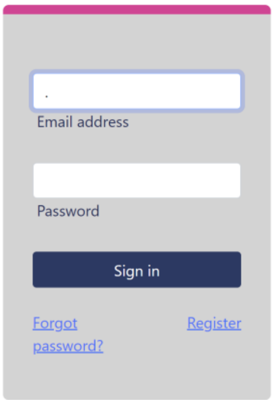
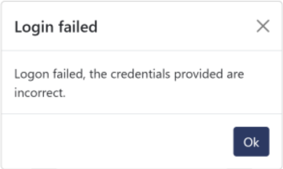
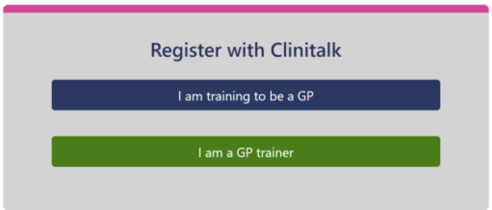
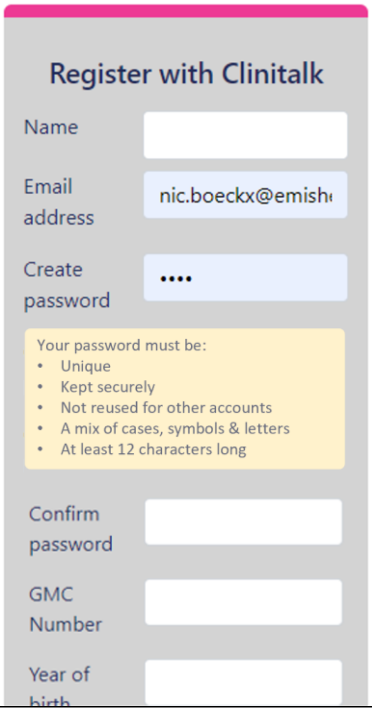
Key personnel:

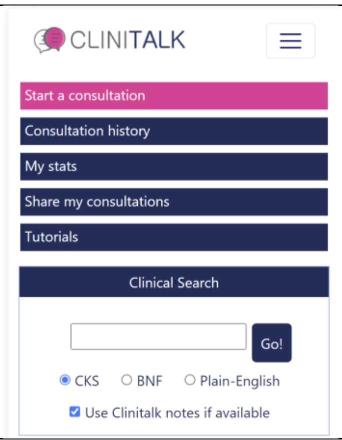
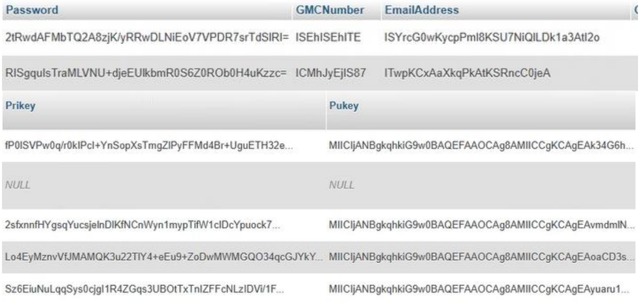
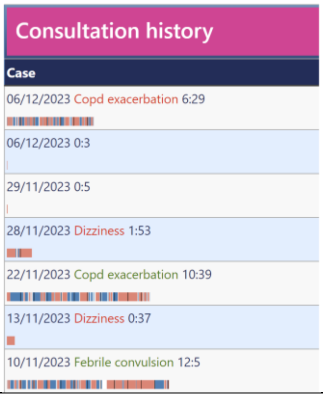
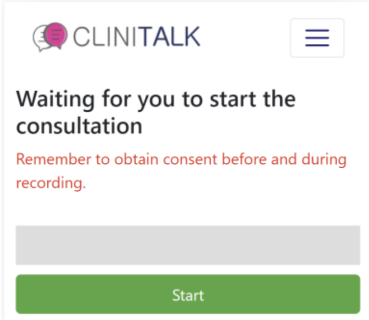
Safety officer, Competencies

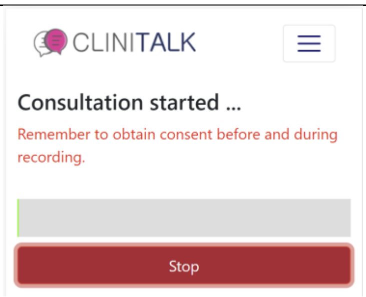
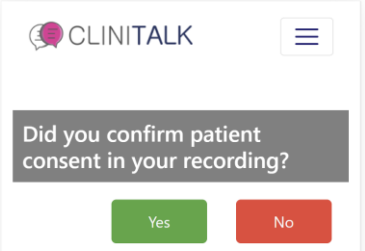
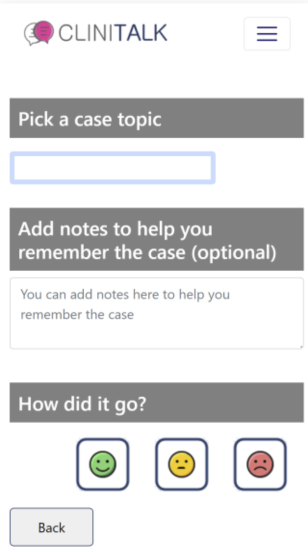
Stage 3 – Purpose (Development)

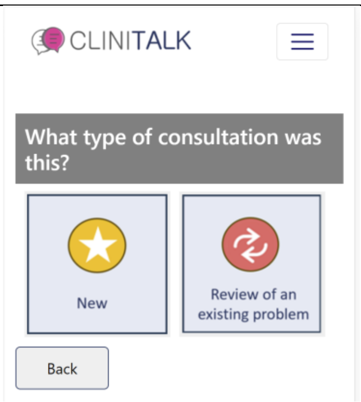
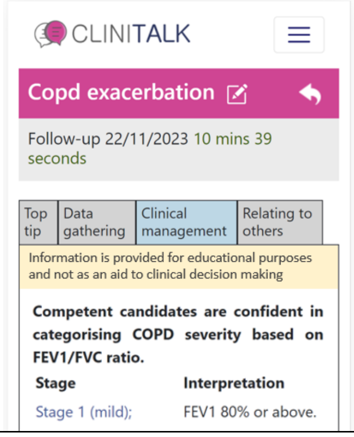
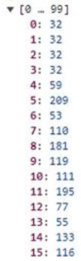
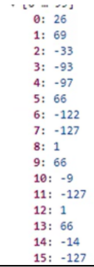
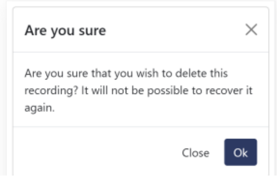
Purpose: The purpose of stage 3 is to develop the solution in line with the design from stage 2, to address the needs identified and to mitigate the associated risks.

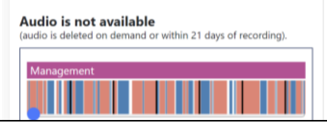
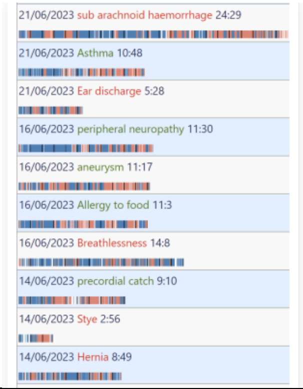
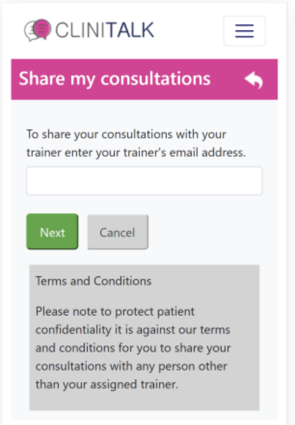
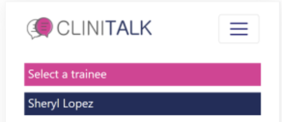
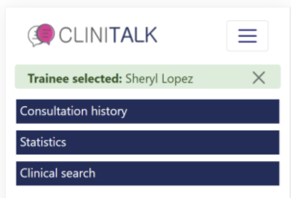
Stage 3 – Feature Testing

Function	Outcome	Evidence	Notes
Login	Success	 . Email address Password Sign in Forgot password? Register  Login failed Logon failed, the credentials provided are incorrect. Ok	Login user with correct credentials – success Prevent login with incorrect credentials – success Protect against brute force attack with exponentially escalating time out - success
Registration	Screen display success	 Register with Clinitalk I am training to be a GP I am a GP trainer	Success
Registration	Screen display success	 Register with Clinitalk Name Email address: nic.boeckx@emish Create password: •••• Your password must be: - Unique - Kept securely - Not reused for other accounts - A mix of cases, symbols & letters - At least 12 characters long Confirm password GMC Number Year of birth	Registration screens display correctly alongside user guidance.

Registration	Account creation success	 CLINITALK Start a consultation Consultation history My stats Share my consultations Tutorials Clinical Search Go! ● CKS ○ BNF ○ Plain-English ☑ Use Clinitalk notes if available	Account registers correctly in database
Database Encryption	Database encryption successful	Sample of encrypted fields  Password · GMCNumber · EmailAddress 2tRwdAFMbTQ2A8zjK/yRRwDLNiEoV7VPDR7srTdSIRI= · ISEhISEhITE · ISYrcG0wKycpPml8KSU7NiQILDk1a3AtI2o RISgquIsTraMLVNU+djeEUlkbmR0S6Z0ROb0H4uKzzc= · ICMhJyEjIS87 · ITwpKCxAaXkqPkAtKSRncC0jeA Prikey · Pukey fP0ISVPw0q/r0kIPcl+YnSopXsTmgZIPyFFMd4Br+UguETH32e... · MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAk34G6h... NULL · NULL 2sfxnnfHYgsqYucsjeInDIKfNCnWyn1mypTifW1cIDcYpuock7... · MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAvmdmIN... Lo4EyMznvVfJMAMQK3u22TIY4+eEu9+ZoDwMWMGQO34qcGJYkY... · MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAoaCD3s... Sz6EiuNuLqqSys0cjgl1R4ZGqs3UBOtTxTnIZFFcNLzIDVi/1F... · MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAyuaru1...	User data encrypted at rest and in transit. Review of fields – encryption successful
Testing end to end encryption access by a user on login	Successful	 Consultation history Case 06/12/2023 Copd exacerbation 6:29 06/12/2023 0:3 29/11/2023 0:5 28/11/2023 Dizziness 1:53 22/11/2023 Copd exacerbation 10:39 13/11/2023 Dizziness 0:37 10/11/2023 Febrile convulsion 12:5	User can log in and view their data correctly using end to end encryption.
Recording a consultation, playback, and displaying feedback.	Successful	Starting a recording  CLINITALK Waiting for you to start the consultation Remember to obtain consent before and during recording. Stopping a recording	User recording screens display correctly, and recording is stored successfully. User is successfully required to confirm patient consent.

		 CLINITALK Consultation started ... Remember to obtain consent before and during recording. Stop Confirming consent  CLINITALK Did you confirm patient consent in your recording? Yes No	
Labelling recording	Success	User assigns case topic  CLINITALK Pick a case topic Add notes to help you remember the case (optional) You can add notes here to help you remember the case How did it go? 🙂 😐 🙁 Back User labels recording type (new/review)	User is successfully shown a screen to label the case topic and self-rate their performance. User is successfully shown a screen to label the case type as a new case or review of an existing case.

		 CLINITALK What type of consultation was this? New Review of an existing problem Back	
Displaying feedback	Successful	Case feedback  CLINITALK Copd exacerbation Follow-up 22/11/2023 10 mins 39 seconds Top tip | Data gathering | Clinical management | Relating to others Information is provided for educational purposes and not as an aid to clinical decision making **Competent candidates are confident in categorising COPD severity based on FEV1/FVC ratio.** **Stage** **Interpretation** Stage 1 (mild); FEV1 80% or above.	Case feedback information displays correctly alongside 'on-label use' warning.
Audio encryption test	Success	Encrypted audio sample from database  ▾ [0 … 99] 0: 32 1: 32 2: 32 3: 32 4: 59 5: 209 6: 53 7: 110 8: 181 9: 119 10: 111 11: 195 12: 77 13: 55 14: 133 15: 116 Same sample unencrypted  0: 26 1: 69 2: -33 3: -93 4: -97 5: 66 6: -122 7: -127 8: 1 9: 66 10: -9 11: -127 12: 1 13: 66 14: -14 15: -127	Audio successfully encrypted. Audio transit and storage encryption successful. De-encryption playback successful
Audio deletion after 21 days or user command	Success	Deletion selected by user  Are you sure × Are you sure that you wish to delete this recording? It will not be possible to recover it again. Close Ok Message showing deletion successful	Audio auto deletion after 21 days. Result confirmed in database. – successful Audio deletion on user demand. Result confirmed in database. – successful.

		 **Audio is not available** (audio is deleted on demand or within 21 days of recording). 	
Consultation recording history display	Success	Consultation history view  21/06/2023 sub arachnoid haemorrhage 24:29 21/06/2023 Asthma 10:48 21/06/2023 Ear discharge 5:28 16/06/2023 peripheral neuropathy 11:30 16/06/2023 aneurysm 11:17 16/06/2023 Allergy to food 11:3 16/06/2023 Breathlessness 14:8 14/06/2023 precordial catch 9:10 14/06/2023 Stye 2:56 14/06/2023 Hernia 8:49	Encrypted consultation history data displays to logged in user. - successful
Share with trainer	Success	Share consultation screen with terms and conditions for on label use.  **Share my consultations** To share your consultations with your trainer enter your trainer's email address. Terms and Conditions Please note to protect patient confidentiality it is against our terms and conditions for you to share your consultations with any person other than your assigned trainer. Post login the trainer screen successfully shows the linked trainee records from shared trainees  Select a trainee Sheryl Lopez Selecting a linked trainee succesfully shows the trainee account.  **Trainee selected:** Sheryl Lopez Consultation history Statistics Clinical search	Public and private key generation (links account and maintains encryption throughout) - successful Record share – successful Trainer view of trainee account - successful

The design was translated into code using coding standards and best practice to implement the necessary features and functionalities. We conducted regular code reviews and tests during development to review functionality and security in line with our procedures and policies.

Report - stage 3 - Risk evaluation

Risks identified:

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

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the hazard log 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.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) 2023 June 2023

Report - stage 4- Testing

System definition:

View here

Version: 1.0

Interoperability:

Clinitalk does not replace or interface with any existing systems.

Clinical risk management system:

Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

Key personnel:

Safety officer, Competencies

Stage 4 – Purpose (Testing)

Purpose: The purpose of stage 4 is to test the solution developed in stage 3, to ensure it addresses the needs identified in stage 2 and mitigates the associated risks.

At stage 4 we perform iterative system testing and regression testing to identify bugs and issues using test data and role played consultations.

Development, Test and Production environments

Four versions of the system are maintained, each of which contains its own database and software environment:

- **Development** – a local environment within which all new development and changes are first made and tested
- **Test** – Software builds from the development environment are first uploaded into the test environment where all changes are tested and then all pre-existing functionality is also tested to ensure no breaking changes have been introduced.
  Pre-release testing conducted in the test environment is documented in the DevOps log as described below.
- **Live** - A production system for use in normal general practice consultations.
- **Examination** - A production system for use in role-played consultations under examination conditions.

Three separate software systems exist for each of these environments:

- Server – Api and database
- Web browser client – Html and JavaScript
- Insights – Rules engine and the rules that it executes.

These systems are tested in isolation (unit testing) and then combined (integration testing) including testing existing functionality to ensure that it has not been broken by recent changes (regression testing).

Pre-release testing

Pre-release testing is formalized to follow a specified methodology which is also revised for each release. This is documented, along with the test results in the DevOps Log spreadsheet.

Regression Testing

Following updates to the code we regression test the following key features:

- Welcome screen displays
- Log in screen displays and login functions
- Multi factor authentication codes generate and send
- Registration fields process correctly
- Registration completes with delivery of verification email
- Account verification completes correctly
- Home screen displays
- Consultation history displays
- Statistics screen displays
- Share screen displays
- Share account function links accounts
- Shared account login functions
- Tutorials screen displays
- Search box displays
- Search dropdown functions
- Search box switch between drugs and case summaries functions
- Search box searches Clinitalk case summaries
- Search screen searches external sources
- Consultation recording screens display

- Consultation recording process functions
- Consultation encrypted storage functions
- Feedback screen loads from consultation history
- Feedback screen scores display
- Feedback screen audio plays
- Feedback screen transcript displays
- Feedback screens delete audio function
- Feedback screen tabs populate with case information

The logs of our regression screen testing are stored in the DevOps log.

Following regression testing we perform system testing.

System Testing

In our system tests we release the completed build to a test environment to verify the complete and integrated software system meets our design requirements. The test includes all components of the build and their interactions and demonstrates the software performs as expected in a real world environment. We test 3 key areas

Functional tests

We test the features listed in the regression testing table to demonstrate they function as an integrated software system within the test environment.

Security tests

We check the integrated software system correctly applies encryption by creating entries and reviewing the encryption applied. We check the decryption by logging in to a user account and reviewing the decrypted entries to check for errors. We make test calls to the Clinitalk API to confirm the API blocks calls to the API that do not originate from the Clinitalk application.

> Note: Prior to live deployment we require a licensed third party to certify security via formal penetration testing. We also require certification of the software development process under cyber security essentials.
>
> Clinitalk cyber essentials security certification
>
> Clinitalk Penetration test certification

Usability tests

We check the integrated system is readily navigable by following the user journey steps outlined in the linked document.

The logs of our system testing are stored in the DevOps log.

User Acceptance Testing

We demonstrate the test build to users and collect feedback on usability and acceptance.

The logs of our user acceptance testing are stored in the DevOps log.

Report - stage 4 - Risk evaluation

Hazard identification, risks identified:

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

No additional risks were identified at stage 4. Hazard identification. The risks identified are described in the hazard log 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.

However following review additional controls were put in place to further mitigate against the risks of off license use including inappropriate sharing of recordings. The additional controls increase the prominence of user warnings. The potential risks and mitigations are listed in the Hazard log table.

- Penetration testing and cyber security essentials testing have been successfully completed.
  - Clinitalk cyber essentials security certification
  - Clinitalk Penetration test certification
- The risks at stage 4 carry a risk rating of between 1 and 2 and are assessed as acceptable to proceed to stage 5.

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.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) 2023 January 2024

Report - stage 5 - Deployment

Purpose: The purpose of stage 5 is to deploy the solution tested in stage 4.

System definition:

View here

Version: 1.0

Interoperability:

Clinitalk does not replace or interface with any existing systems.

Clinical risk management system:

Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

Key personnel:

Safety officer, Competencies

Deployment process

Steps for deployment to the live environment:

1. Backup existing deployment ready for use in roll back in the event of a deployment failure.
2. Review the system configuration requirements and make necessary changes.
    a. System configuration may be required where a release involves changes to the database structure or content.
3. Review the testing information for the new version from the test environment including any system configuration tests.
    a. Testing must follow the testing procedures outlined in stage 4 and our associated policies i.e. change management policy.
4. Check release to the live environment has been signed off.
5. Deploy the new version to the live environment.
6. Complete post deployment checks
    a. Re-run of the regression and system tests documented in the testing phase.
7. Sign off the deployment or roll back the version in the event of deployment failure.
    a. Note deployment tests in the test environment should make roll back in the live environment a rare or never event. If a roll back occurs a roll back report shall be completed with root cause analysis.

System configuration

Our web-based application has no end user hardware, software, environment, or network configuration requirements for deployment.

Deployment may involve changes to the structure and content of the database, and then involves copying the set of new system files into one of the two production environments. Since these two steps are dependent on one another, where database changes are required, the systems must first be taken down temporarily by deleting all the old application and API files, so that the database cannot be used while the changes are taking place. The new versions of these files can then be copied safely into place. At each deployment the need for system configuration is to be reviewed in preparation for release to the live environment.

Version history and Roll Back

A copy of all files included with each release is kept as a record of the release process, and to enable roll-back in the event of some unexpected calamity that prevents a particular version being allowed to remain or fixed. (Note that this is such a rare occurrence that it should never happen). As part of the deployment process if the deployed version fails the deployment testing the deployment team shall roll back to the prior version.

The version of release is recorded in the About section of the released version which is accessed via the main menu.

Deployment scheduling

- 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 our website.

Report - stage 5 - Risk evaluation

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the hazard log 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.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) 2023 February 2024

Report - stage 6 - Maintenance

Purpose: The purpose of stage 6 is to maintain the deployed the solution to ensure ongoing functionality, security, and performance.

System definition:

View here

Version: 1.0

Interoperability:

Clinitalk does not replace or interface with any existing systems.

Clinical risk management system:

Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

Key personnel:

Safety officer, Competencies

Monitoring system functionality and performance

We monitor system performance daily as part of the development operations task list which is monitored and updated by our senior information risk officer. As a part of system monitoring, we log all user activity including user log in and failed user log in attempts and internal system errors. An investigation shall be commenced if an investigation trigger is found.

In addition to the systematic monitoring of system performance we monitor our email inbox for user queries relating to user experience and investigate reports of issues. We keep a member of our team as an active user as an additional performance.

Triggers for investigation

- User reporting of an error.
- Abnormal increase in traffic across a single or multiple users
- Abnormal decrease in traffic across platform users
- Abnormal increase in failed log in attempts.
- System error reported in the log.

Investigation format

An investigation shall use the following format:

Cause :

- The cause shall be labelled categorised as known or unknown and details documented.

Hazards and risk level:

- The incident shall be considered against the hazards listed in the hazard log and the applicable hazards documented alongside a categorisation of risk as per the Clinitalk risk matrix.

Actions:

- The actions required shall be documented as follows:
  - Resolved
    - for incidents where the root cause has been identified, risk is low, and no further actions is required.
  - Further investigation
    - for incidents where the root cause has not been identified the risk is low and further investigation is required.
  - Urgent investigation
    - for incidents where the root cause has not been identified and risk is medium and further investigation is required.
  - Critical incident
    - for incidents where the risk is high and urgent further investigation is required.

Relevant policies:

- Security Incident policy
- Disaster recovery plan
- Information Security Management System
- Information Security policy

Monitoring security

We monitor security via:

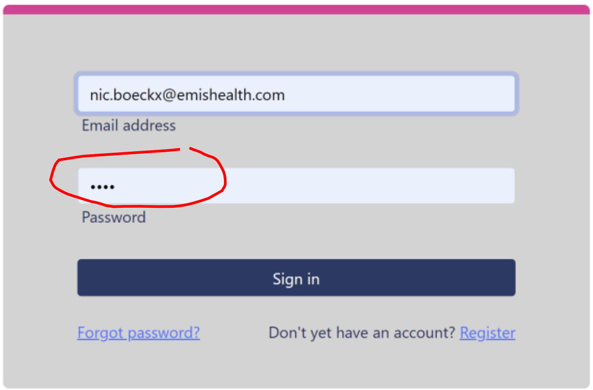
- Daily user activity logs for suspicious activity.
- Penetration testing audits by certified external bodies
- Security audits by certified external bodies.

We maintain security standards via:

- Annual training on data security policies
- Incident response planning
- Monitoring reports of emerging threats – DevOps Threats log

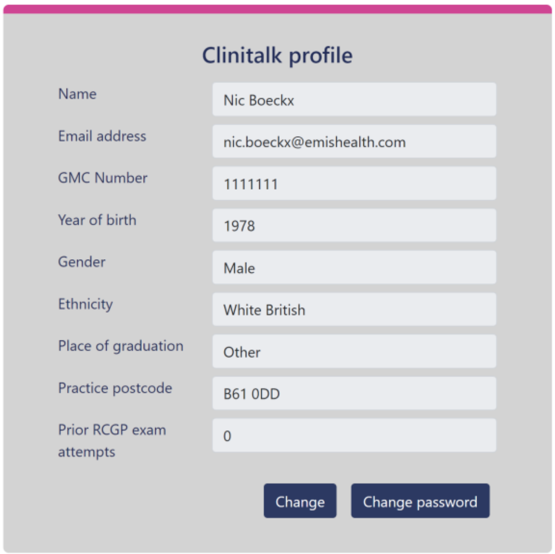
User support

Users can self-serve account issues such as password resets and updates to user details through the login screen ‘forgot password?’ link and post login via their ‘my profile’ page.



Email address: nic.boeckx@emishealth.com

Password: ••••



Clinitalk profile

Name	Nic Boeckx
Email address	nic.boeckx@emishealth.com
GMC Number	1111111
Year of birth	1978
Gender	Male
Ethnicity	White British
Place of graduation	Other
Practice postcode	B61 0DD
Prior RCGP exam attempts	0

Other support items are dealt with via our support email address: info@clinitalk.co.uk

Routine updates, patches, and improvements

Routine updates, patches and improvements are released as described in our deployment process.

Report - stage 6 - Risk evaluation

Hazard identification, risks identified:

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

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the hazard log 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 6 - QA and Sign off:

Dr N.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) 2023 February 2024

Report - stage 7 - Change management

Purpose: The purpose of stage 7 is to plan for the controlled release of updates, enhancements, and bug fixes.

System definition:

View here

Version: 1.0

Interoperability:

Clinitalk does not replace or interface with any existing systems.

Clinical risk management system:

Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

Key personnel:

Safety officer, Competencies

Controlled release of updates, enhancements, and bug fixes

Our controlled release plan is documented in our change management documentation.

Report - stage 7 - Risk evaluation

Hazard identification, risks identified:

1. Off label use
2. Server attack

3. Password attack
4. Sub processor attack
5. Recording without consent
6. Service down
7. Inappropriate sharing of recording

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the hazard log 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 7 - QA and Sign off:

Dr N.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) 2023 February 2024

Report - stage 8 - End of life

Purpose: The purpose of stage 7 is to plan for the controlled release of updates, enhancements, and bug fixes.

System definition:
View here

Version: 1.0

Interoperability:
Clinitalk does not replace or interface with any existing systems.

Clinical risk management system:
Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

Key personnel:
Safety officer, Competencies

End of life strategy

Our controlled end of life plan will minimize disruption, address user concerns, and maintain a positive relationship with our users and stakeholders.

1. Notification and Communication:

- We will provide advance notice to users, stakeholders, and relevant parties 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:

- We will clearly outline the process for handling user data. This may include providing users with options to export their data or outlining how the data will be securely deleted after the shutdown.

- We will ensure compliance with data protection regulations and privacy policies during the data transition or deletion process.

3. Service Availability:

- We will specify the date on which the web application will be taken offline and communicate any service downtime or interruptions to users and stakeholders.

4. Support and Customer Service:

- We will handle user inquiries and issues via our standard email contact address during the end-of-life period as well as posting information on the login page and our website.

5. Documentation:

- We will update documentation to reflect the end-of-life status. This includes updating the website, knowledge base, and any other resources users might consult.

6. Archiving:

- We will archive the application's codebase, databases, and relevant documentation in a secure location.

- We will ensure that future stakeholders can access historical information if needed.

7. Legal and Compliance Considerations:

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

8. Financial Considerations:

- We will communicate any financial implications, such as refunds for users who have paid for the application or its services.

- We will outline the process for handling financial transactions during the end-of-life period.

9. Internal Communication:

- We will inform internal teams, including developers, support staff, and other relevant personnel, about the end-of-life plan.

- We will provide guidance on their roles and responsibilities during the shutdown process.

10. Closure Announcement:

- We will issue a final announcement to officially close Clinitalk and express gratitude to users and stakeholders for their support throughout the application's .

Report - stage 8 - Risk evaluation

Hazard identification, risks identified:

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

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the hazard log 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 8 - QA and Sign off:

Dr N.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) 2023 February 2024

Report - stage 9 - Documentation and compliance

Purpose: The purpose of stage 9 is maintaining accurate documentation and ensuring compliance with relevant regulations.

System definition:

View here

Version: 1.0

Interoperability:

Clinitalk does not replace or interface with any existing systems.

Clinical risk management system:

Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

Key personnel:

Safety officer, Competencies

Documentation of the life cycle

The Clinitalk life cycle is documented in the following sections of this document:

Clinitalk system development lifecycle

Introduction Reports stages organized by lifecycle stage.

Product description by lifecycle stage

Audits

The audits, policies and documentation that document our regulatory compliance are listed and accessible here.

Report - stage 9 - Risk evaluation

Hazard identification, risks identified:

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

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the hazard log 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 9 - QA and Sign off:

Dr N.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) 2023 February 2024

Report - stage 10 - Review and continuous improvement

Purpose: The purpose of stage 10 is to assess the effectiveness of the Clinitalk system and to make improvements.

System definition: View here

Version: 1.0

Interoperability: Clinitalk does not replace or interface with any existing systems.

Clinical risk management system: Clinitalk risk management process, Review of risk, Risk management plan, Clinitalk governance structure

Regular Reviews

Our controlled release plan is documented in our change management documentation.

At our triannual 4 monthly review meetings in April, August, and December we review metrics of our effectiveness in the following categories:

- User feedback, positive and negative
- Usage statistics (number of active users, number of sessions, user retention, numbers of new users)
- Reliability (down time)
- Performance (page load times, audio processing times)
- Error logs
- Security – review of any security incidents
- Costs – processing and maintenance costs
- Regulatory compliance – changes in the regulatory landscape
- Scalability – server load

The content of the report is business sensitive and therefore a link to it is not provided.

We continuously monitor system performance and user requests as documented in lifecycle stage 6.

Improvements are made via our change management process. We review change requests at our weekly board meetings and apply the change management processes documented in lifecycle stage 7.

Report - stage 10 - Risk evaluation

Hazard identification, risks identified:

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

Hazard identification. No additional risks were identified at this stage. The risks identified are described in the hazard log 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.Boeckx (Data Protection Officer), Dr P Salmon (Product Safety Officer) 2023 February 2024

4.1 Clinical risk analysis process

The clinical safety officer has ensured that the risk management activities outlined in the clinical risk management plan have been implemented. All areas involved in the development and maintenance of the product have been involved in the risk analysis including representatives from the following:

Product safety officer

Data protection officer

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.

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 and December 2023 workshop.

Hazards are documented in our 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 in the risk management plan. The estimation of risks is documented in the hazard log table.

The assessment of severity scale is documented here.

The assessment of likelihood scale is documented here.

The two-dimensional risk matrix is documented here.

5.1 Risk evaluation

For each individual hazard the acceptability of the initial risk has been evaluated and documented in the 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.

The definitions of risk acceptability are documented here.

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. 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. 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

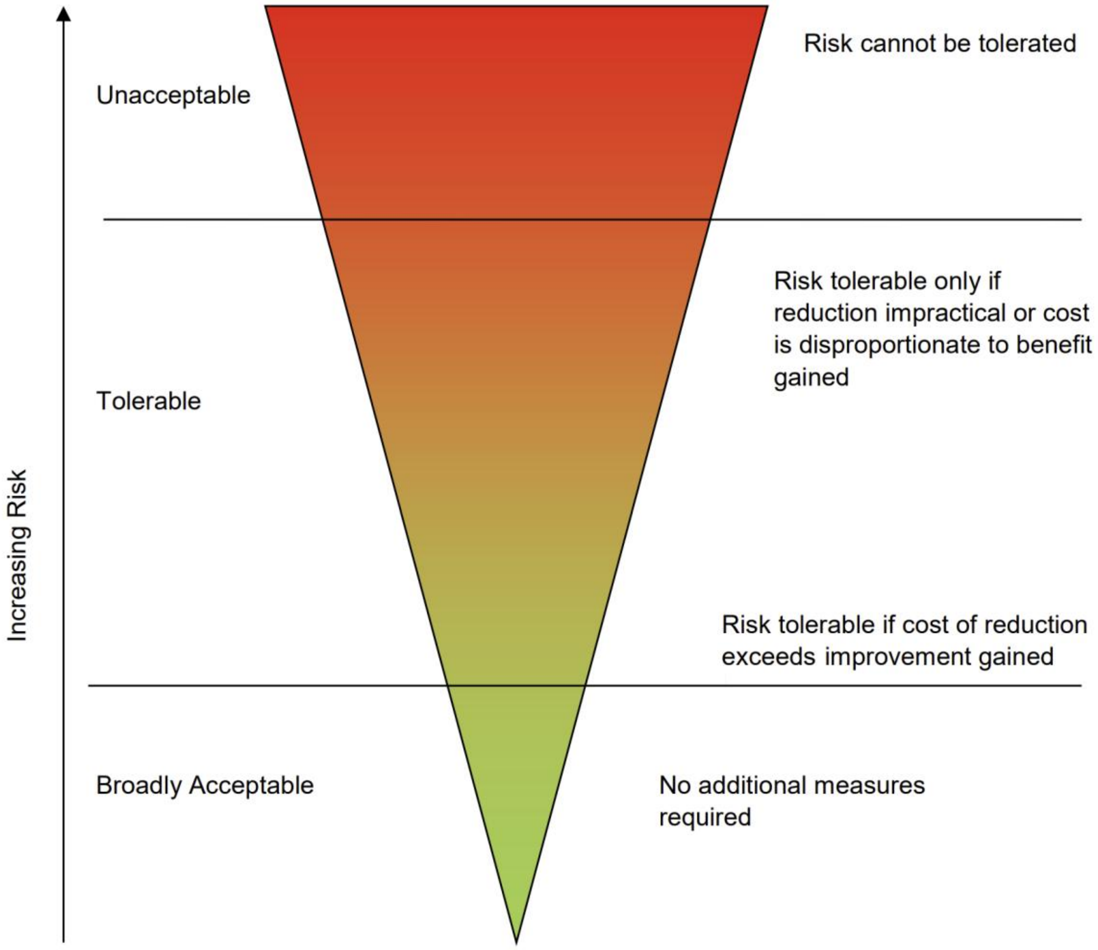
Risk benefit is required for every hazard where the residual risk is deemed as unacceptable and further risk control is not practicable. As stated in 6.1 the current risk assessment state is that no unacceptable residual risks have been identified and therefore additional risk benefit analysis has not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


Increasing Risk
Unacceptable
Risk cannot be tolerated
Tolerable
Risk tolerable only if reduction impractical or cost is disproportionate to benefit gained
Risk tolerable if cost of reduction exceeds improvement gained
Broadly Acceptable
No additional measures required

6.3 Implementation of clinical risk control measures

The clinical risk control measures documented in the 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. Other evidence such as logs, audits, and certification can be found in the resources list. 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 and the accompanying the 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. 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 incident log which is maintained and regularly reviewed as part of our weekly team updates and triannual review meetings.

Our security incident policy outlines our procedures for monitoring and responding to safety incidents.

We keep logs of:

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

We will monitor user logs each working day as part of our development operations task list which is monitored and updated by our senior information risk officer. Our logs are stored in the incident log.

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

All logged and reported items relating to safety concerns must be stored and processed via the incident log according to our security incident policy.

The impact of safety concerns must be documented in the incident 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 and documented in the safety case reports.

Incidents must be reported and resolved in a timely manager as per our security incident policy.

The validity of any assumptions and the effectiveness of any controls made in the Safety Case Report are monitored via the incident log to ensure the perceived level of clinical risk remains representative and acceptable. If it is found that the Safety Case does not hold in live system use, then Clinitalk will undertake the risk activities described in Sections 4 to 6 of the standard. This may result in additional or modified risk control mechanisms being introduced to manage the risk. Any such changes are to be recorded in a re-issued Safety Case Report.

Users may be notified and updated of a safety incident via email and or via notices posted on the user log in screen.

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 extent 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