# CLINITALK Information Security Management System

**Change control**

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer | Date | Comments | Version |
| N.Boeckx | 25/9/23 | ISMS review | 1.0 |
| N.Boeckx | 1/4/2024 | ISMS review  | 1.1 |
| N.Boeckx | 11/4/2025 | ISMS review  | 1.2 |

Next review date: April 2025

Contents

CLINITALK Information Security Management System 1

Context 1

Organisational Aims (ISO 27001 section 4.1) 2

Interested parties and requirements (ISO 27001 section 4.2a and b) 2

Suppliers 6

Scope (ISO 27001 section 4.3) 6

Description of the scope: 7

Boundaries of the ISMS 7

Exclusions from the ISMS: 8

Applicability 8

Establishing, implementing, maintaining and continually improving ISMS (ISO 27001 section 4.4) 9

Policies and Key Documents 9

General Principles 11

Risk assessments 12

Process 12

Data access 12

Identified risks 12

Context

See DPIA ‘Purposes of System/Process’ found here 1000 Clinitalk Data Protection Impact Assessment

Clinitalk’s purpose is to help trainees, training schemes and ultimately patients by improving the delivery of medical training for UK General Practice (GP). Our innovative digital solution addresses the pressing need in the UK for more trainee mentoring in response to high patient demand, lack of human resource and the costs of scaling. By analysing consultation audio using our innovative insights engine we generate post consultation feedback. Our feedback helps trainees to capitalise on their learning opportunities by stimulating the kind of personal reflection a GP trainer might provoke were they able to sit in on every consultation. In doing so we calculate performance data that enables training programs to remotely monitor the progress of trainees and thereby identify and address training issues early. Data sharing is necessary because Clinitalk requires audio diarisation and transcription services to convert audio into an input it can process. Data is held by our sub processor for the minimum time necessary to complete processing and typically between 1 and 60 seconds per request. No audio or transcript data is stored in the data processing service.

The solution supplies GP trainees with access to computer generated post consultation educational feedback about their communication skills alongside key case related clinical knowledge for every consultation, to help them learn to effectively deliver information and resources that empower patients in the management of their health problems.

Intended Benefits:

By improving the delivery of medical training, we hope to support the drive to increase the number and quality of GPs available to provide health services to the UK population.

The practice benefits from additional training support and ability to monitor the trainee progress. Trainees benefit from the additional training support and feedback. Patients benefit from the additional training received by their doctors and the improved consulting skills that result.

Data Collected:

Consultation audio. User registration data. Data required to process payments.

With patient and trainee consent, the data collected is an encrypted audio recording of the consultation between the GP trainee and the consented patient. The time and date of a recording is stored with the recording, but written patients details are not stored. Clinitalk also collects demographic information about the user to tailor feedback to the user and to create a user account. Data collected includes the GP trainees GMC number, email, ethnicity, prior exam attempts, country of graduation, sex. At the request of the GP trainee and with patient consent, Clinitalk provides an efficient and secure method of analysing, encrypting and storing consultations which may include personal and special category information. Stored data is deleted within 21 days of a consultation, or earlier at the users command. Data is stored and processed in compliance with the requirements of the UK-General Data Protection Regulations (UK-GDPR) and the Data Protection Act (2018)

## Organisational Aims (ISO 27001 section 4.1)

The organisational aims are set out in our information security policy statement found here: 1007 Information security policy

## Interested parties and requirements (ISO 27001 section 4.2a and b)

The people organisations laws and frameworks with an interest in Clinitalk’s data security systems include:

|  |  |  |  |
| --- | --- | --- | --- |
| Interested Party | Requirement and Source | Comments | Relevant documents |
| All customers | **Requirement**: Data must remain under UK GDPR control **Source**: GDPR articles | All stakeholders require assurance that their data is processed legally (explicit consent) and securely with respect for their data rights under UK GDPR regulation.  | 1000 Data Protection Impact Assessment and in 1024 Privacy notice. |
| All customers | **Requirement**: Our data processing must be lawful, fair, and transparent to the data subject.**Source**: GDPR articles | All customers require that we clearly communicate our business purpose to our interested parties and demonstrate that our data processing is lawful, ethical, and beneficial. | 1000 Data Protection Impact Assessment and 1024 Privacy notice. |
| All customers | **Requirement**: Data we collect must be collected for specified, explicit, and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.**Source**: GDPR articles | All customers require that we explicitly state the reason for our data collection and limit it to that necessary for our business purpose. | 1000 Data Protection Impact Assessment and 1024 Privacy notice. |
| All customers | **Requirement**: All stakeholders require that data collected by us should be relevant, and limited to what is necessary in relation to the purposes for which they are processed.**Source**: GDPR articles | We must limit data collection to that necessary for our business purpose. | 1000 Data Protection Impact Assessment and in 1024 Privacy notice and 1015 Consent and storage policy |
| All customers | **Requirement**: All stakeholders require that personal data we hold must be accurate and up to date. Inaccurate data should be rectified or erased without delay**Source**: GDPR articles | We are responsible for ensuring we keep accurate records and correct inaccuracies. This applies to the three types of data we hold user data, patient data, and employee data.  | 1000 Data Protection Impact Assessment and in 1024 Privacy notice. |
| All customers | **Requirement**: Data should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.**Source**: GDPR articles | We are responsible for ensuring we minimise the storage of sensitive data. | 1000 Data Protection Impact Assessment and in 1024 Privacy notice. |
| All customers | **Requirement**: Personal data must be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.**Source**: GDPR articles | We are responsible for ensuring we process data securely and protect that data against unauthorised access and loss. | 1011 Disaster recovery plan, 1007 Information security policy, 1000 Data Protection Impact Assessment, 1005 Data Processing Agreement Assembly, and in 1024 Privacy notice |
| All customers | **Requirement**: Data must not be transferred outside the EU/UK unless UK GDPR transfer mechanisms are in place such as an international adequacy agreements or standard contractual clauses.**Source**: GDPR articles | We have an international sub processor. When we transfer data internationally to our sub processor we must ensure it is done under the UK GDPR standard contractual clauses. | 1005 Data Processing Agreement Assembly, and in 1000 Data Protection Impact Assessment. |
| All customers | **Requirement**: Demonstrate accountability and governance principles in compliance with the principles of GDPR. **Source**: GDPR articles | We are obliged to comply with the principles of GDPR by implementing appropriate policies and controls. In this information security management document, we list the policies and procedures that demonstrate our compliance. | This document. |
| All customers | **Requirement**: Demonstrate compliance with data subject rights.**Source**: GDPR articles | Data subjects have several rights that we must be mindful of, including the right to be informed, right of access, right to rectification, right to erasure (right to be forgotten), right to restrict processing, right to data portability, right to object, and rights related to automated decision making and profiling. We have assessed the rights of our data subjects in our DPIA documentation, and we are committed to compliance with these requirements. | 1000 Data Protection Impact Assessment. |
| All customers | **Requirement**: Maintain prompt data breach reporting. **Source**: Data processing agreement customer | All stakeholders expect a robust response to data breach. We have implemented a reporting target of 4 hours from discovery. | 1013 Security incident policy.docx |
| All customers | **Requirement**: Service uptime of 99%**Source**: Data processing agreement customer | Our stakeholders require reliable service that maintains data availability and integrity. We have addressed service uptime in our policies and processing agreements. We aim to provide service uptime of >99% through our processing agreements. | 1033 Data Processing agreement customer |
| All customers | **Requirement**: Demonstrate a disaster recovery plan for data restoration **Source**: Data processing agreement customer | Our stakeholders require a plan for recovery of service and outlines the procedures, responsibilities and actions required in response to any unauthorised or unexpected event that threatens the security or integrity of our systems and assets. | 1011 Disaster recovery plan.docx |
| All customers | **Requirement**: Demonstrate audits of services to ensure compliance with NHS requirements including cyber essentials, data penetration testing, data security reviews, asset register and NHS Digital Technology Assessment criteria.**Source**: Data processing agreement customer | Patients and customers require assurance that their data is processed legally (explicit consent) and securely with respect for their data rights under UK GDPR regulation. We have consulted with patients during pilot and asked for opinion across a range of patient groups. We have consulted with trainees, and trainers during pilot and asked for opinion regarding their requirements. We have consulted with Health Education England and the RCGP during pilot and investigated their requirements. We have also consulted with the integrated care board assurance framework team Dudley and reviewed the NHS Digital Technology Assessment criteria.  | 1033 Data processing agreement customer, 1027 Digital Technology Assessment Criteria, 1004 Cyber essentials compliance summary, 1018 Asset register and Audits, 1031 Penetration testing documentation |
| Internal staff | **Requirement**: Train and update staff on our information security management system and processes.**Source**: Internal data security policy | Our team are an essential part of our information security management system and require appropriate guidance, training and resources. We have consulted with our team members about how we use data and how to provide appropriate guidance and resource. | 1022 Annual training on data security policies |
| Clinitalk shareholders and management | **Requirement**: Provide clear policies and procedures to NHS digital standards**Source**: Management target | Our management requires the team to provide clear policies and procedures for all required standards to facilitate a systematic approach to information security and product development.  |  |
| NHS Customers | **Requirement**: Asset register**Source**: NHS digital cyber essentials requirements | NHS standards require that we hold asset registers of our information assets, and software and firmware assets so we understand our security risks and put in place security measures. | 1018 Asset register and Audits |
| NHS Customers | **Requirement**: Record of processing activities**Source**: NHS digital cyber essentials requirements | NHS standards require a record of our processing activities so we can assess and monitor our processing of data to ensure compliance with UK GDPR legislation. | 1018 Asset register and Audits |
| NHS Customers | **Requirement**: Appropriate technical measures to protect against cyber attack**Source**: NHS digital cyber essentials requirements | NHS standards require that we employ appropriate technical measures to protect against cyber attack as outlined in the NHS digital cyber essentials requirements. | 1004 Cyber essentials compliance summary, 1007 Information security policy, 1008 Password Protection Policy, 1009 Database Credentials Policy, 1010 Cryptography Control Policy, 1014 Access control policy |
| NHS Customers | **Requirement**: User account processes internal and external**Source**: NHS digital cyber essentials requirements | NHS standards require that we have robust user account processes that govern the use of our services. | 1016 User registration policy, 1025 Internal User registration policy, 1012 Acceptable use policy |

## Suppliers

Companies that supply services to Clinitalk may also come into contact with information held by Clinitalk. It is therefore essential that they maintain the same high standards of information security that Clinitalk does.

These suppliers include:

* TechnicalConsulting.uk
* Microsoft Azure
* Assembly AI
* Open AI

## Scope (ISO 27001 section 4.3)

 This scope section is also included in ‘1007 Information security policy’

This section outlines the scope of the Information Security Management System (ISMS) in accordance with ISO/IEC 27001for Clinitalk, a browser-based application designed to record consultation data for educational purposes.

**Scope Change Control**

|  |  |  |
| --- | --- | --- |
| Reviewer | Date | Comments |
| N.Boeckx | 4/10/2023 | Scope review |
| N.Boeckx | 1/4/2024 | ISMS review  |
| N.Boeckx | 11/4/2025 | ISMS review  |

### Description of the scope:

The ISMS applies to the entire lifecycle of Clinitalk, including the development, operation, maintenance, and support phases. It covers the collection, storage, processing, and transmission of consultation data within the application.

Boundaries of the ISMS

The ISMS encompasses all information assets, resources, and processes related Clinitalk and included but is not limited to the following:

|  |  |  |
| --- | --- | --- |
| Boundary | Details | Additional information |
| Locations in scope: | Internal locations:* Clinitalk UK office Worcestershire
* Clinitalk UK office Hazelmere

Outsourced locations:* Microsoft azure
* Assembly AI
* Open AI
 | Customers require assurance that internal and outsourced locations apply appropriate technical and physical security standards. |
| Internal Processes in scope: | 1. Development and testing environments
2. 2Operational environment (Data processing and storage)
3. Maintenance & Support
4. Security processes (database credentials, cryptography, password protection, acceptable use, access control, penetration testing.
5. Payment processes
6. GDPR compliance processes (DPIA)
7. Incident response processes (Disaster recovery, incident response)
 |  |
| Outsourced Processes in scope (External suppliers with access to our information assets): | Assembly AI (Transcription and diarisation)Azure (Cloud storage)OpenAI (Anonymised data processing) |  |
| Personal data in scope: | Information assets covered by this ISMS include: Consultation data, User data, Payment data, Intellectual property, Employee records | 1018 Information asset register (Record of processing activities) |
| Other Assets in scope | Hardware, application databases, storage systems, software. | see information asset register for more detail - 1018 Information asset register |
| Organisation units in scope: | Relevant parts of Clinitalk in scope: Management, Development, Commercial and Personnel | In scope are all management policies and procedures including data protection impact assessments, access control, annual training, personnel register, user registration, hazard logs, annual training, security incident, disaster recovery, cyber essentials compliance. |
| Functions in scope: | Payments  |  |
| Regulatory and legal requirements in scope: | GDPR, Cyber essentials. |  |
| Employees and roles in scope: | Management, developers. | This includes employees at all levels who handle, process, or have access to sensitive information. |

Exclusions from the ISMS:

The following aspects are explicitly excluded from the scope of this ISMS certification:

* User-owned devices and networks used to access the application
* Third-party services and applications

Applicability

This ISMS is applicable to all employees, contractors, and third-party service providers who have access to the data within Clinitalk. It covers all locations where the product is developed, deployed, or maintained.

## Establishing, implementing, maintaining and continually improving ISMS (ISO 27001 section 4.4)

Clinitalk affirms our commitment to the establishment, implementation, maintenance, and continual improvement of out information security management system to the standard within the scope of our ISMS as described in section 4.3. Our requirements are detailed in section 4.2a and b. Our policies, processes, and audits are designed around those requirements and demonstrate our established processes, their implementation, maintenance, and improvement. To meet our requirements, we have put in place a number of controls that safeguard, manage, mitigate or eliminate security risks pertaining to our requirements. These are documented in our policies and key documents which are outlined below.

# Policies and Key Documents

The Clinitalk Information Security Management System includes a set of policies and key documents that are intended to ensure that the requirements of this system are met for the benefit of all interested parties.

Key documents and their location are listed in the file ‘Index of Key documents file’ and below:

## General Principles

Inevitably the storage and management of data exposes potential vulnerabilities that can be exploited in malicious ways. The objective of this policy is therefore to minimise such vulnerabilities to make access to this data extremely difficult for anyone attempting to do so maliciously, whilst ensuring that the integrity of the data is maintained to enable genuine and honest access to it to continue.

1. Data should only be collected and stored if there is a good reason to do so.
2. When data is no longer needed it should be deleted.
3. All locations where such data may be stored should be accessible only with the knowledge of a ***strong*** password.
4. Where the actual value of a datum is not of ongoing value a hash of the data should be stored in its place.
5. Data that is required should be backed up regularly to ensure its ongoing availability in the case of a failure concerning the primary source.
6. Such backups should also be stored in a secure location, only accessible with a strong password.
7. Users are restricted from installing unsigned applications.
8. Access permissions should be tailored to the individuals role and activity. Access to administrator accounts should be used only for necessary activities. It is prohibited to use administrator accounts for day to day activities.