# Access Control Policy for Clinitalk Clinical System

**Change control**

|  |  |  |  |
| --- | --- | --- | --- |
| Reviewer | Date | Comments | Version |
| N.Boeckx | 25/9/23 | Admin controls policy updated | 1.0 |
| N.Boeckx | 1/4/24 | Admin controls policy updated | 1.0 |
| N.Boeckx | 11/04/2025 | Admin controls policy updated | 1.0 |
|  |  |  |  |
|  |  |  |  |

Next review date: April 2026

Contents

[Access Control Policy for Clinitalk Clinical System 1](#_Toc146523503)

[1. Purpose 1](#_Toc146523504)

[2. Scope 1](#_Toc146523505)

[3. Access Control Principles 2](#_Toc146523506)

[4. Access Control Mechanisms 2](#_Toc146523507)

[5. Training and Awareness 3](#_Toc146523508)

[6. Compliance and Enforcement 3](#_Toc146523509)

[7. Policy Review 3](#_Toc146523510)

[8. Administrator account processes 4](#_Toc146523511)

[a) Policy Communication: 4](#_Toc146523512)

[b) User Account Management: 4](#_Toc146523513)

[c) Administrator Account Management: 4](#_Toc146523514)

[d) Education and Training: 4](#_Toc146523515)

[e) Monitoring and Auditing: 4](#_Toc146523516)

# 1. Purpose

The purpose of this access control policy is to ensure the confidentiality, integrity, and availability of patient data within the Clinitalk clinical system. This policy outlines the principles and guidelines for granting, managing, and revoking access to patient data by authorized personnel.

# 2. Scope

This policy applies to all individuals and entities that have access to the Clinitalk clinical system, including healthcare professionals, administrative staff, and technical support personnel.

# 3. Access Control Principles

a. Principle of Least Privilege: Access privileges will be granted based on the principle of least privilege. Users will be granted the minimum access necessary to perform their job responsibilities effectively.

b. Need-to-Know: Access to patient data will be granted only to authorized individuals who have a legitimate need-to-know to fulfil their job responsibilities.

c. Role-Based Access Control (RBAC): Access privileges will be assigned based on job roles and responsibilities. Users will be granted access to specific functionalities and patient data based on their assigned roles.

d. Separation of Duties: Sensitive actions, such as access to code dealing with encryption, transit and storage or granting access privileges, will be separated among different individuals to prevent unauthorized or inappropriate use.

e. Access Revocation: Access privileges will be promptly revoked when an individual's job responsibilities change, or when they no longer have a need-to-know for patient data.

f. Authentication and Authorization: All users accessing the Clinitalk clinical system must authenticate their identity using unique credentials (e.g., username and password). Authorization will be granted based on the user's role and access requirements.

# 4. Access Control Mechanisms

a. User Accounts: Each user will have a unique user account tied to their individual identity. User accounts will be created, modified, and deactivated by the system administrator or designated personnel.

b. Password Management: Users will be required to create strong passwords, which must be changed periodically. Passwords should not be shared, and password reuse is strictly prohibited.

c. Role-Based Access Control (RBAC): Access privileges will be assigned based on predefined roles. The system administrator or designated personnel will manage role assignments and ensure they align with users' job responsibilities.

e. Audit Logs: The Clinitalk clinical system will maintain audit logs of user activities, including logins, access attempts, and data modifications. Audit logs will be regularly reviewed to detect any unauthorized access or suspicious activities.

f. Encryption: Patient data transmitted over the network and stored within the system will be encrypted using industry-standard encryption algorithms to protect confidentiality and integrity.

# 5. Training and Awareness

All personnel with access to the Clinitalk clinical system will receive comprehensive training on their roles and responsibilities regarding data access, privacy, and security. No staff will be issued with administrator accounts without completing training and an appropriate security vetting at recruitment. Regular awareness programs will be conducted to keep staff informed about the importance of adhering to the access control policy.

# 6. Compliance and Enforcement

Non-compliance with this access control policy may result in disciplinary action, including but not limited to warnings, suspension of access privileges, or termination of employment. Any suspected security breaches or policy violations should be reported immediately to the appropriate authority.

# 7. Policy Review

This access control policy will be reviewed annually or as needed to ensure its effectiveness and alignment with evolving technology, legal, and regulatory requirements.

By following this access control policy, Clinitalk aims to safeguard patient data, prevent unauthorized access, and maintain the privacy and security of healthcare information within the clinical system.

Roles based access to source code:

Clinitalk team access:

Pete Salmon – Role – developer - access to Clinitalk code environment for development and maintenance

Nic Boeckx – no source code access required

# 8. Administrator account processes

Ensuring that employees do not use administrator accounts for day-to-day activities like browsing the internet and checking emails is an important security and operational practice. Administrator accounts should be reserved for system maintenance, configuration, and other privileged tasks.

## a) Policy Communication:

All staff members will be advised on our administrator access and use policy during onboarding and annually.

## b) User Account Management:

 - Create Standard User Accounts: All employees will be provided with standard user accounts with appropriate permissions for their job roles.

 - Annual review of privileges: We annually review and restrict the permissions of standard user accounts to limit unnecessary access rights. Spreadsheet link Tab: Annual data security review

## c) Administrator Account Management:

 - Centralized Control: We maintain strict control over administrator accounts, limiting their distribution to only essential personnel. Our head of technology (Peter Salmon) is responsible for the provision of administrator accounts.

## d) Education and Training:

 - Security Training: We provide annual training on our policies to help employees understand the importance of not using administrator accounts for everyday tasks.

 - Technical Training: We train administrators on proper security practices and secure alternatives to achieve their tasks without using admin accounts.

## e) Monitoring and Auditing:

 - Regular Auditing: We conduct annual audits to help identify instances of administrator accounts being used for non-admin tasks including a review of operating system logging and alerting to monitor unusual or unauthorized account activity.