GDPR Compliance Audit for Clinitalk

Ensuring Data Protection and Privacy

# Introduction

At Clinitalk, we are committed to ensuring the highest standards of data protection and privacy. As part of this commitment, we have undertaken an audit to ensure our compliance with the General Data Protection Regulation (GDPR). This audit covers a review of our contracts, policies, and data processing activities, reflecting our dedication to protecting the personal data of our customers and stakeholders.

# Scope of the Audit

The audit encompasses the following key areas:

* Contracts: We have reviewed all our contracts to ensure they align with GDPR requirements, including clauses on data protection, data processing agreements, and third-party vendor compliance.
* Policies: Our internal policies have been scrutinised and updated to ensure they meet GDPR standards. This includes our data protection policy, privacy policy, and procedures for handling data breaches.
* Data Processing: We have assessed our data processing activities, ensuring that all personal data is handled in compliance with GDPR principles. This includes data minimisation, lawful processing, and secure storage.

# Audits of Compliance in dcb0129

As part of our ongoing commitment to GDPR compliance, we have conducted audits of compliance in dcb0129. These audits have confirmed that our practices are in line with GDPR requirements, and we have taken necessary steps to address any identified gaps.

# Penetration Testing and Cybersecurity Essentials Plus Certification

To further ensure the security and protection of personal data, we have been externally audited by CREST certified penetration testing to identify and mitigate vulnerabilities in our systems. Additionally, we have achieved the Cybersecurity Essentials Plus certification, demonstrating our commitment to robust cybersecurity measures.

# Audited documents

### Information Security & Data Protection

- Data Protection Impact Assessment

- Information Security Management System

- Information Security Policy

- Password Protection Policy

- Database Credentials Policy

- Cryptography Control Policy

- Disaster Recovery Plan

- Security Incident Policy

- Access Control Policy

- User Registration Policy

- Internal User Registration Policy

- Data Processing Agreement Assembly

- Data Processing Agreement Customer

- Data Security and Protection Toolkit

- Change Management Policy

- Audits GDPR Compliance Audit

- ISO27001 ISMS Requirements Review

- Penetration Testing Documentation

### Compliance & Legal

- Non Disclosure Agreement - Assembly AI

- Non Disclosure Agreement Template

- Cyber Essentials Compliance Summary

- GDPR Compliance Audit

- ICO Self Assessment Tool

- Clinical Risk Management File

- Medical Device Assessment

- Privacy Notice

- Data Coord Board Compliance Assessment

### Technology & Systems

- EV Code Signing Certificate

- Digital Technology Assessment Criteria

- DevOps Log

- Clinitalk Workplan Evidence

### Policies & Procedures

- Acceptable Use Policy

- Consent and Storage Policy

- Asset Register & Audits

- Key Dates

- Incident Log

- Design Process Summary

- Contract and Service Level Agreement

- Business Continuity Exercise

### Training & Analysis

- Annual Training on Data Security Policies

- Training Needs Analysis Summary

- Personnel Register

- Content Authoring Policy

### Assurance & Frameworks

- Integrated Care Board Assurance Framework

# Assessment for 2024

These assessments have confirmed that our practices, policies, and contracts meet GDPR standards, and we are fully compliant.

# Assessment for 2025

Our 2025 assessments have confirmed that our practices, policies, and contracts continue to meet GDPR standards, and we are fully compliant.

# Conclusion

Clinitalk remains dedicated to maintaining the highest standards of data protection and privacy. Our GDPR compliance audit reflects our commitment to safeguarding personal data and ensuring the trust of our customers and stakeholders. We will continue to monitor and improve our practices to ensure ongoing compliance with GDPR and other relevant data protection regulations.