Clinical Computing (UK) Ltd
Mediqal Health Informatics Ltd

Information Security Policy

Effective Date:	**10th July 2023**
Document Reference:	**I-POL-0001**
Review:	**Next review July 2024**

clinicalcomputing MEDIQAL HI.

Contents

1 Introduction 3

1.1 Purpose 3

1.2 Policy Objectives 3

1.3 Definitions and abbreviations 4

1.4 Associated documents 4

2 Roles and responsibilities 4

1 Introduction

1.1 Purpose

Clinical Computing UK Ltd and Mediqal Health Informatics Ltd, who provide, maintains and supports an electronic medical record system for the management of information applicable to chronic kidney disease , is committed to preserving the confidentiality, integrity and availability of all assets, including personally identifiable information (PII), in scope of the information security management system (ISMS) in order to compete in the marketplace and maintain its legal, regulatory and contractual compliance and commercial image.

Clinical Computing UK Ltd and Mediqal Health Informatics Ltd are committed to ensuring compliance with all applicable legislative, regulatory and contract requirements, including all applicable PII protection legislation.

To achieve this, Clinical Computing UK Ltd and Mediqal Health Informatics Ltd have jointly implemented an ISMS in accordance with the international standard ISO/IEC 27001:2013. The ISMS is subject to continual, systematic review and improvement.

In the remainder of this document The Company means Clinical Computing UK Ltd and Mediqal Health Informatics Ltd.

1.2 Policy Objectives

- Information is made available to all authorised parties with minimal disruption to the business processes.
- Information security and privacy risks are managed.
- The integrity of this information is maintained.
- Confidentiality of information is preserved.
- Regulatory, legislative and other applicable requirements related to information security are met.
- Appropriate information security and privacy objectives are defined and measured.
- Appropriate business continuity arrangements are in place to counteract interruptions to business activities and these take account of information security.
- Appropriate information security and privacy education, awareness and training is available to staff and relevant others, e.g. suppliers, working on behalf of The Company.
- Breaches of information security or privacy and security incidents, actual or suspected, are reported and investigated through appropriate processes.
- Appropriate access control is maintained and information is protected against unauthorised access.
- Continual improvement of the ISMS is made as and when appropriate.
- This procedure applies to all documents and records required by The Company ISMS and must be followed by all staff of The Company.
- Commitment to achieving, supporting and managing compliance with all applicable PII legislation, including the contractual terms agreed between The Company and its clients.

1.3 Definitions and abbreviations

Term	Definition
ISMS	Information Security Management System
QMS	Quality Management System – ISO 13485 Medical Device Quality Management System implemented by Clinical Computing UK Ltd.
PII	Personally identifiable information (PII) is information that, when used alone or with other relevant data, can identify an individual.

1.4 Associated documents

Document reference	Title
I-MAN-0001	Information Security Manual
BS EN ISO 27001:2017	Information technology – Security techniques – Information security management systems - Requirements

2 Roles and responsibilities

Information Security Manager is accountable for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

All employees and those working under the scope of the ISMS are expected to comply with this policy and with the ISMS that implements this policy. The consequences of breaching the Information Security Policy are set out in The Company's disciplinary policy and in contracts and agreements with third parties.

The Company has established an Information Security Team chaired by the Managing Director to support the ISMS framework and to periodically review the Information Security Policy.