DOCUMENT NUMBER: CL02	**VERSION NUMBER:** 2.0
CREATION DATE: 16/05/2022 **PUBLICATION DATE:** 16/05/2022	**NUMBER OF PAGES:** PAGE 1 OF 4
TITLE: Managing Patient Data	**Security Classification:** Restricted

AMENDMENT RECORD

VERSION NUMBER	DATE	CHANGE
0.1	15/12/2018	Initial draft
1.0	26/08/2021	Final version
2.0	16/05/2022	Update content and new template format (previous UM-IS-1003)

DOCUMENT OWNER:	NAME: Chris Broderick	DATE: 16/05/2022
QUALITY APPROVAL:	NAME: Teresa Latta	DATE: 16/05/2022

1. PURPOSE

The purpose of this procedure is to detail the correct method for how uMed securely manages patient data according to legislation, regulations of where the study and/or recruitment is taking place and the contract between uMed and the client.

2. SCOPE

This procedure explains the different controls in place that must be followed to ensure patient data management is followed correctly. This document should be complemented with any other information security policies that form part of the uMed Integrated Management System.

3. RESPONSIBILITIES

All uMed staff working in the different stages of a project that may involve patient data will be responsible for carrying out this procedure. The CTO will oversee that all staff will work in accordance with this document.

4. DEFINITIONS

Terminology	***Definition***
SOP	Standard Operating Procedure
CTO	Chief Technology Officer

5. TRAINING AND COMPETENCY

Training on this document will be reading and acknowledging this procedure and complemented with GDPR, HIPAA and security awareness training.

6. RELATED DOCUMENTS

GEN06-Information Classification, labelling and handling SOP
IT02-Access Control Policy
IT10-IT Acceptable Use Policy (AUP)
IMS01-Information security Policy
MS09-Confidentiality Policy
IMS10 Managing incidents procedure

7. HEALTH AND SAFETY

None

8. PROCEDURE

uMed may access patient data from medical infrastructure(s) such from GP's and NHS digital; through internal applications that have permission to connect and query patient data.

8.1. General Access Control and Handling Rules

1. Access must only be given by job role need and/or signed off by the line manager.
2. Access should not be given until staff completes induction mandatory training.
3. Access should be removed if no longer needed or immediately after working hours on the last leaving day.
4. Access must comply with privileged accounts rules.
5. Exported data must always be encrypted with GP encryption with a minimum 2048 bit keys.
6. It is not permissible to download patient data to a local computer unless it is appropriately encrypted.
7. Screenshots of identifiable patient data are not permitted.

8.2. Infrastructure Configuration and Server Access Controls

Valid reasons for accessing the infrastructure configuration in production:

1. Debugging infrastructure deployment issues.
2. Deploying or upgrading infrastructure.

In both instances a log should be maintained for audit trail purposes.

The following personnel are permitted ongoing access to production infrastructure

1. The Chief Technology Officer.
2. Head of Engineering.
3. Production Development Deployment Engineer.

Short term access can be granted to engineers who have necessary security training and are signed off for access by the CTO or head of Engineering. The following process must always take place when granting short term access to any personnel, if:

1. The access is time boxed and removed soon after that expires.
2. Extension time follows the same sign off process as initial granted permission.

8.3. User Interface Application Access Controls

1. Access must only be given by job role need and/or signed off by the line manager.
2. Access should not be given until staff completes induction mandatory training.
3. Access should be removed if no longer needed or immediately after working hours on the last leaving day.
4. Access must comply with privileged accounts rules.
5. Exported data must always be encrypted with GPG encryption with a minimum 2048 bit keys.
6. Access must comply with privileged accounts rules.
7. Exported data must always be encrypted with GPG encryption with a minimum 2048 bit keys.
8. It is not permissible to download patient data to a local computer unless it is appropriately encrypted and there is an associated business reason.

9. Screenshots of identifiable patient data are not permitted.

8.4. Application Server Access Controls

Valid reasons for accessing the infrastructure configuration in production:

1. Debugging infrastructure deployment issues.
2. Deploying or upgrading infrastructure
3. Fixing data issues.

The following personnel are permitted ongoing access to production infrastructure

1. The Chief Technology Officer.
2. Head of Engineering.
3. Designated operations staff authorised by the Head of Commercial Operations for ongoing data management and issue support.

Short term access can be granted to engineers who have necessary security training and are signed off for access by the CTO or the Head of Engineering; if following the time boxed access rules in section Infrastructure Configuration and Server Access Controls.

8.5. Data Security Procedures

Any data ingested into the platform or files created for export must conform with the following rules:

1. Data at rest must be encrypted.
2. All decryption keys must be stored securely in a key manager or secret store.
3. Secret and decryption keys must be encrypted if being transported to the destination server(s) that use them.

8.6. Data Handling Procedures

Data handling shall follow uMed Information Classification, labelling and handling SOP (GEN06) and any incidents shall follow Managing incidents procedure (IMS10).

9. RECORDS

None

10. APPENDICES

None