



DOCUMENT NUMBER: IMS09		VERSION NUMBER: 1	
CREATION DATE: 04/05/2022 PUBLICATION DATE: 05/05/2022		NUMBER OF PAGES: PAGE 1 OF 4	
TITLE: Confidentiality Policy		Security Classification: Restricted	
AMENDMENT RECORD			
VERSION NUMBER	DATE	CHANGE	
1	04/05/2022	First publication	
CONTENT OWNER:	NAME: Chris Broderick	DATE: 04/05/2022	
QUALITY APPROVAL:	NAME: Teresa Latta	DATE: 05/05/2022	
This procedure is a mandatory requirement and forms part of the uMed Integrated Management System (IMS) Amendments are only permitted via the change control procedure			
UNAUTHORISED COPIES OF THIS DOCUMENT ARE NOT PERMITTED			

DOCUMENT NUMBER:	IMS09	VERSION NUMBER:	1
CREATION DATE:	04/05/2022	NUMBER OF PAGES:	PAGE 2 OF 4
TITLE:	Confidentiality Policy		

1. PURPOSE

The purpose of the Confidentiality Policy is to ensure that all employees and users understand uMed requirements in relation to the disclosure of personal data and confidential information.

2. SCOPE

The scope of this policy, confidentiality relates to the transmission of personal, sensitive or identifiable information about individuals or organisations (confidential information), which comes into the possession of uMed through its work.

uMed holds personal data about its staff, users, clients and contractors that will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside or inside of the organisation without prior permission.

3. RESPONSIBILITIES

Managers (or HR) that onboard new employees have the responsibility to communicate this policy to employees at the induction process and thereafter if the policy is updated.

All uMed staff, contractors and 3rd Parties shall adhere to this policy.

4. DEFINITIONS

<u>Terminology</u>	<u>Definition</u>
DPO	Data Protection Officer
ICO	Information Commissioner's Office
DBS	Disclosure and Barring Services

5. TRAINING AND COMPETENCY

Training on this policy will be achieved by reading and acknowledging this document.

6. RELATED DOCUMENTS

IMS10 - Data Protection Policy

GEN06 - Information Classification, Labelling, Handling and Disposal

7. HEALTH AND SAFETY

None

DOCUMENT NUMBER:	IMS09	VERSION NUMBER:	1
CREATION DATE:	04/05/2022	NUMBER OF PAGES:	PAGE 3 OF 4
TITLE:	Confidentiality Policy		

8. CONFIDENTIALITY

As a legal term, *confidentiality* refers to a duty of an individual to refrain from sharing confidential information with others, except with the express consent of the other party, except under certain specific circumstances.

9. LEGAL AND REGULATORY FRAMEWORK

uMed are governed by legislation to process personal data, confidential sensitive data, and corporate data legally and ethically.

The main United Kingdom legislative instruments are:

- Human Rights Act 1998
- Data Protection Act 2018
- UK General Data Protection Regulation
- Common Law Duty of Confidentiality in Health and Social Care
- Access to Medical Reports Act 1988

The main United States of America legislative instruments are:

- Health Insurance Portability and Accountability Act 1996
- Children's Health Insurance Authorization Act of 2009
- Patient Safety and Quality Improvement Act 2005

10. POLICY ELEMENTS

Confidential and proprietary information is defined as secret, valuable, expensive, information / data that may be easily replicated. Common examples of confidential information are:

- Employee Personal data.
- Unpublished financial information.
- Data of Clients/Contractors.
- Customer lists (existing and prospective).
- Data entrusted to the company by external parties.
- Pricing/marketing and other undisclosed strategies.
- Documents and processes explicitly marked as confidential.
- Unpublished goals, forecasts and initiatives marked as confidential.

Common examples of confidential sensitive information are:

- Patients' data
- Patents, formulas, or new technologies.
- Genetic or biometric data.

Employees may have various levels of authorised access to confidential and confidential sensitive information.

DOCUMENT NUMBER:	IMS09	VERSION NUMBER:	1
CREATION DATE:	04/05/2022	NUMBER OF PAGES:	PAGE 4 OF 4
TITLE:	Confidentiality Policy		

10.1. What employees should do:

- Always lock or secure confidential information in a safe place.
- Avoid printing confidential documents, but if necessary, shred those documents as soon as they are no longer needed.
- Ensure that confidential information is always stored in a secure environment or on secured devices.
- Only disclose confidential / sensitive information to other employees when it is necessary and authorised.
- Keep confidential documents inside the company's premises/digital network unless it is necessary to move them.

10.2. What employees shouldn't do:

- Use confidential information for any personal benefit or profit.
- Disclose confidential information to anyone outside of our company.
- Replicate confidential documents and files and store them on unsecured devices.

When employees stop working for our company, they are obliged to return any confidential files and delete them from their personal devices/drives.

10.3. Confidentiality Measures

We will take measures to ensure that confidential information is well protected by:

- Store and lock any paper documents that can not be converted into a digital format..
- Encrypt electronic information and safeguard databases.
- Ask employees/contractors to sign confidentiality as part of their contract of employment/NDA/SLA.
- Ask for authorization by senior management to allow employees to access certain confidential information if required.

10.4. Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons. Examples are:

- If a regulatory body requests such information as part of an investigation or audit
- If our company examines a venture or partnership that requires disclosing some information (within legal boundaries)

In such cases, employees involved should document their disclosure procedure and collect all needed authorizations.

10.5. Disciplinary Consequences

Employees who do not adhere to our confidentiality policy will face disciplinary and, possibly, legal action.

11. INTELLECTUAL PROPERTY

This policy also applies to all and any Intellectual Property owned by the Company, created by employees in accordance with their work for the uMed and/or created by contractors in accordance with the terms of their work for the Company.

Such Intellectual Property shall form part of the Company's confidential information and this policy shall apply in full to the Intellectual Property.

Employees/contractors to sign intellectual property as part of their contract of employment/NDA/SLA.