DOCUMENT NUMBER: IMS06	**VERSION NUMBER:** 1
CREATION DATE: 09/06/2022 **EFFECTIVE DATE:** 09/06/2022	**NUMBER OF PAGES:** PAGE 1 OF 7
TITLE: Data Protection Policy	**Security Classification:** Unrestricted

AMENDMENT RECORD

VERSION NUMBER	DATE	CHANGE
1	09/06/2022	First publication

DOCUMENT OWNER:	NAME: Matt Wilson	DATE: 09/06/2022
QUALITY APPROVAL:	NAME: Teresa Latta	DATE:09/06/2022

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

1.0 PURPOSE

The purpose of this policy is to describe how personal data must be collected, handled and stored to meet the uMed data protection standards and comply with relevant legislation, including the General Data Protection Regulations (GDPR).

2.0 SCOPE

This Policy applies to all systems, people and processes that constitute the organisation's information systems, including directors, employees, suppliers and other third parties who have access to uMed systems.

3.0 RESPONSIBILITIES

Data Protection Officer (DPO) has the following responsibilities:

- Briefing the Board of Directors on Data Protection responsibilities
- Reviewing Data Protection and related policies and additional documentation
- Notification to the Information Commissioner's Office (ICO) and Directors of any incidents
- Handling subject access requests
- Review and approving unusual or controversial disclosures of personal data

Chief Technology Officer (CTO) has the following responsibilities:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards
- Performing regular checks and scans to ensure security hardware and software is functioning properly
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services

Head Of Quality & Compliance is responsible for the following:

- Providing and maintaining data protection documents
- Advising Directors and staff on Data Protection issues
- Ensuring that Data Protection induction and training takes place
- Review and approving contracts on data protection
- Addressing any data protection queries from stakeholders
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles
- Ensure consent is obtained
- Handling subject access requests on behalf of the DPO
- Log and investigate any data incidents

All staff

- Responsibility for ensuring that data is collected, store and handled appropriately
- Responsibility to ensure any incidents are immediately reported to the DPO and the Head of Quality & Compliance

4.0 DEFINITIONS

Terminology	***Definition***
Data subject	Person who is identified or who could be identified, directly or indirectly (including by reference to a name, an identification number, location data, or various other factors).
Personal data	Any information (including opinions and intentions) which relates to a data subject
Controller	Person or organisation who or which (whether alone or jointly with others) determines the purposes and means of the Processing of Personal Data.
Processor	Person or organisation who or which Processes Personal Data on behalf of the Controller
Process	It is given a very wide meaning under the GDPR and includes any operation or set of operations which is performed on Personal Data (whether or not by automated means) and includes collecting, recording, organising, adapting, retrieving, erasing and even just storing Personal Data
Data Breach	It is breach of security leading to the accidental or unlawful destruction, loss or alteration of Personal Data, or unauthorised disclosure of or access to Personal Data.
DPO	Data Protection Officer
ICO	Information Commissioner's Office
SAR	Subject Access Request

5.0 TRAINING AND COMPETENCY

Training in this procedure will be achieved by reading this SOP.

6.0 RELATED DOCUMENTS

IMS09- Confidentiality Policy
IIMS01- Information Security Policy
IMS08- Data Protection Impact Assessment Procedure
IMS05- IS Breaches and Near Misses Workflow and Log

7.0 HEALTH AND SAFETY

None

8.0 POLICY

When acting as Data Controller or Data Processor[1] uMed is committed to:

- Complying with data protection law and following good practice
- Providing training and support for staff and contractors who handle personal data, so that they can act confidently and consistently
- Being open about how individuals' data is stored and processed
- Protecting itself from the risks of data incidents
- Respecting and protecting individuals' rights
- Being open and transparent with individuals whose data is held

In addition to being open and transparent, uMed will be open and transparent and will seek to give individuals and clients as much choice as is possible and reasonable over what data is held on them and how it is used.

As enforced by the UK GDPR UK, all data will;

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection as this is agreed with clients

This data may include but is not limited to:

- Names of Individuals
- Postal Addresses
- Email Addresses
- Telephone Numbers
- Payroll Records
- Absence Records
- Medical Records
- DBS
- Plus, any other relevant information relating to individuals that is required in the delivery of a service or in adherence to a contractual or legal obligation that we have with relevant authorities or our clients, suppliers or partners.

uMed has identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (information being given out inappropriately)
- Insufficient clarity about the range of uses to which data will be put — leading to Data Subjects being insufficiently informed
- Failure to offer choice about data use when appropriate

[1] Most of the activities with clients uMed is acting as data Processor only

- Breach of security by allowing unauthorised access
- Failure to establish efficient systems of managing changes, leading to personal data being not up to date
- Harm to individuals if personal data is not up to date
- Insufficient clarity about the way personal data is being used e.g. released to the general public
- Failure to offer choices about use of contact details for staff, clients, clients employees, contractors
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data

8.1 ACCESS TO PERSONAL DATA ('SUBJECT ACCESS REQUEST-SAR')

Any subject access requests will be handled by the Data Protection Officer that will delegate the management of requests to the Head of Quality & Compliance.

All individuals who are the subject of personal data held by uMed are entitled to:

- Ask **what information** the company holds about them and why
- Ask **how to gain access** to it
- Be informed **how to keep it up to date**
- Be informed how the company is **meeting its data protection obligations**

uMed always verifies the identity of anyone making a subject access request before handing over any information. This verification should be made of **two** documents to prove identity and proof of address (example a driving licence and a utility bill).
The data will be provided within one month from the day the requester identity is validated.

8.2 INDIVIDUAL RIGHTS TO PRIVACY

Umed has a GDPR Privacy Statement relating to the services, setting out how data relating to individuals is used by the company, which can also be found on the website.

8.3 RIGHT OF ERASURE

All individuals have the right to have data erased, commonly referred to as the right to be forgotten.

We have the right to refuse to erase data where this is necessary in the right of freedom of expression and information, to comply with a legal obligation for the performance of a public interest task, exercise of an official authority, for public health purposes in the public interest, for archiving purposes in the public interest, scientific research, historical research, statistical purposes or the exercise or defence of legal claims. In case of lawful refusal, the requester will be advised of the grounds of our refusal, the right to complain to the ICO or other accreditors and/or regulators and the right to seek judicial remedy.

8.4 RIGHT OF RECTIFICATION

All individuals have the right to have data corrected if it contains inaccuracies.

We have the right to refuse to rectify data where the request is manifestly unfounded or excessive considering whether the request is repetitive in nature.

8.5 RIGHT TO RESTRICT

All individuals have the right to have our processing activities restricted where the individual contests the accuracy of the data (until the accuracy is verified), where the individual objects to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) and where we are considering whether our organisation's legitimate grounds override the individual's interests.

This right does not prevent uMed processing the data by way of storage, to establish and exercise a legal claim, to establish or defend a legal claim or where processing is necessary to protect the rights of another individual or organisation.

We have the right to refuse to rectify data where the request is manifestly unfounded or excessive considering whether the request is repetitive in nature.

8.6 RIGHT TO DATA PORTABILITY

Individuals have the right to data portability in that they may obtain and reuse their data for their own purposes across different services, from one IT environment to another in a safe and secure way, without hindrance to usability. This applies where data is processed on the grounds of consent, performance of a contract or by automated means.

The exact method will change from time to time and will be determined and notified at the time of the request.

We have the right to refuse the request where it is manifestly unfounded or excessive, considering whether the request is repetitive in nature.

8.7 RIGHT TO OBJECT

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

It is anticipated that the second category above, will not apply to uMed as we do not currently have a direct marketing system.

8.8 TIME-LIMITS, REFUSALS AND FEES

Under GDPR, individuals have the right to access, request erasure, rectification, and the restriction of their data without charge. These requests need to be processed within one month of receipt/identify verification. In exceptional cases, this may be extended to three months, but the Data Protection Officer shall advise the requester of this delay within the first month after the request.

Where any decision is taken to refuse to comply with all or part of a request, the Data Protection Officer shall advise the requester of this and advise of the requester's right to complain to the Information Commissioner's Office within the first month after the request.

In other special circumstances, the uMed may have the right to charge a fee where the request is manifestly unfounded or excessive. Reasonable fees shall be notified to the individual together with the grounds of imposing a fee, the right to complain to the ICO or other accreditors and/or regulators and the right to seek judicial remedy.

8.9 MAKING, RECEIVING AND PROCESSING REQUESTS

This section concerns Subject Access Requests, Rectification, Erasure, Restriction, Portability or Objection.

Individuals are entitled to make such requests and should do so by contacting the DPO by email at dpo@umed.io. Current and former employees are also entitled to make such requests and should do so by contacting the DPO.

Such requests made from individuals outside the company should be encouraged to be submitted by email, addressed to the DPO with their request and specific points regarding their request. If any employee receives such a request directly, it should be immediately forwarded to the DPO. If an employee receives such a request by telephone or verbally, the employee should encourage the request to be made by email to the DPO and, if they refuse, notify the DPO immediately.

9.0 RECORDS

IMS06_A-Data Subject Access Request Log

10.0 APPENDICES

None