Data protection policy

Table of Contents

1) INTRODUCTION

a) Purpose and scope

The aim of this Policy is to ensure that Micropathology Ltd complies with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679); Data Protection Act 2018, the Caldicott2 report March 2013 (previously Caldicott 1997) and the ICO.

This policy aims to clarify the principles that govern all uses (any processing, paper or electronic) of Micropathology Ltd information assets, in particular patient identifiable and confidential information and staff personal data (irrespective of its nature (health and non-health related), and to ensure that certain practices are adhered to.

It is designed to protect the privacy and confidentiality of patients, staff and other members of the public. It seeks to strike a balance between the privacy rights of the individual whose information is being used (known as the data subject) and the sometimes competing interests of those with legitimate reasons for using personal information.

This policy is applicable to all staff, contractors, students and volunteers working within Micropathology Ltd or processing data on behalf of the company onsite or elsewhere.

The company is registered with the Information Commissioner's Office as an organisation that processes personal data.

b) Responsibility

The Micropathology Ltd Data Protection Officer, Dr Colin Fink, has the accountability for the application of this policy within the company and its annual review.

It is the responsibility of all staff, contractors, students and volunteers processing data on behalf of Micropathology Ltd to comply with this policy.

Acknowledgement of this obligation is recorded in iPassport – the Company Quality Management System electronic database, employment contracts, confidentiality statements or contractual documentation with third parties (e.g. information sharing agreements, data processor contracts, service level agreements, etc.).

It is the duty of the Quality Manager to ensure that document control procedures are followed. All staff performing this procedure are responsible for ensuring that they understand and follow procedures. The Quality Manager and training officer should ensure that personnel are trained and competent in the procedures.

c) Reason for revision

Removal of Pete Matthews and added further information in regard to how personal data is treated and how new starters are informed. Changed archiving of personal data to six years. Amended reference from Prof Fink to Dr Fink. Amended reference to Cyber Essentials Plus Certificate of Assurance to correctly reference iPassport entry.

2) HEALTH AND SAFETY

Not applicable.

3) PROCEDURE

a) Definitions

Company	means Micropathology Ltd, a registered company.
GDPR	means the General Data Protection Regulation.

b) Policy principles

Statutory Requirements

There are legal and ethical requirements for Micropathology Ltd to protect identifiable and confidential information processed by or on behalf of the company as their roles as data controllers and processors. This includes any technical and organisational security measures required to preserve the confidentiality, integrity and availability of the information on which its operations depend.

Personal Data

Personal data is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

Data protection principles

The company is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

The GDPR seeks to strike a balance between the privacy rights of the individual whose information is being used (known as the data subject) and the sometimes competing interests of those with legitimate reasons for using personal information.

The Caldicott principles

The 7 Caldicott principles are:

Principle 1: Justify the purpose for using confidential information

Every proposed use or transfer of personally identifiable information, either within or from an organisation, should be clearly defined and scrutinised. Its continuing uses should be regularly reviewed by an appropriate guardian.

Principle 2: Don't use personal confidential data unless absolutely necessary

Identifiable information should not be used unless it's essential for the specified purposes. The need for this information should be considered at each stage of the process.

Principle 3: Use the minimum necessary personal confidential data

Where the use of personally identifiable information is essential, each individual item should be considered and justified. This is so the minimum amount of data is shared and the likelihood of identifiability is minimal.

Principle 4: Access to personal confidential data should be on a strict need-to-know basis

Only those who need access to personal confidential data should have access to it. They should also only have access to the data items that they need.

Principle 5: Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and their obligation to respect patient and client confidentiality.

Principle 6: Understand and comply with the law

Every use of personally identifiable data must be lawful. Organisations that handle confidential data must have someone responsible for ensuring that the organisation complies with legal requirements.

Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients and within the framework set out by these principles. They should also be supported by the policies of their employers, regulators, and professional bodies.

Accountability

Processing: This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Micropathology Ltd holds large amounts of confidential information, most of which relates to and identifies patients and employees of the service. This information should be treated

with respect to ensure confidentiality, integrity and availability of the information, so it is accessible when and where needed by those with a legitimate need for it.

c) What type of data processor is Micropathology Ltd?

The GDPR draws a distinction between a 'controller' and a 'processor' in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. The GDPR defines these terms:

Controllers

'**Controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

This means the company is responsible for complying with the GDPR and must be able to demonstrate compliance with the data protection principles, and take appropriate technical and organisational measures to ensure data processing is carried out in line with the GDPR.

Controllers make decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.

Example

A GP surgery uses an automated system in its waiting room to notify patients when to proceed to a GP consulting room. The system consists of a digital screen that displays the waiting patient's name and the relevant consulting room number, and also a speaker for visually impaired patients that announces the same information.

The GP surgery will be the controller for the personal data processed in connection with the waiting room notification system because it is determining the purposes and means of the processing.

Processors

P**rocessor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

As a processor, the company have more limited compliance responsibilities. Processors act on behalf of and under the authority of the relevant controller (For example our users). In doing so, the company serves the controller's (Our users) interests rather than the company's.

Example

A gym engages a local printing company to produce invitations to a special event the gym is hosting. The gym gives the printing company the names and addresses of its members from its member database, which the printer uses to address the invitations and envelopes. The gym then sends out the invitations.

The gym is the controller of the personal data processed in connection with the invitations. The gym determines the purposes for which the personal data is being processed (to send individually addressed invitations to the event) and the means of the processing (mail merging the personal data using the data subjects' address details). The printing company is a processor processing the personal data only on the gym's instructions.

Micropathology Ltd are both a data processor and data controller.

d) Data register

To ensure its processing of all data is lawful, fair and transparent, the company shall maintain a Data Register. The Data Register is regularly updated (responsibility of Weiping Barrett and Pete Millichap) and shall be reviewed at least annually. Individuals have the right to access their personal data and any such requests made to the Data Protection officer shall be dealt with in a timely manner.

e) Lawful purposes of data processing

All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests. The company shall note the appropriate lawful basis in the Data Register of Systems. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the company's systems.

The privacy notices for staff outline the purposes and use of personal data and staff are

given a clear explanation of how it will be treated and the way information might be shared on the first day of employment.

For the provision of care, the company does not require any explicit consent of patients as detailed in Article 6 (e) of the GDPR 'processing is necessary for the performance of a task in the public interest' and article 9 (h) 'processing is necessary for the preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health and social care or management of health and social care services'. For secondary use / non-care provisions, where the use of information is not involved in direct care, then a specific legal basis for that use must exist. This means that the company is not permitted to use patient data as it sees fit and subjects must be informed about:

- Use and disclosure of information and records
- Choices they have and the implications an limitations regarding the sharing of data.

f) Data minimisation

The company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

g) Accuracy

The company shall take reasonable steps to ensure data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that data is kept up to date.

h) Archiving / removal

To ensure that personal data is kept for no longer than necessary, the company shall retain personnel data for a total of six years after cessation of employment. Patient data is held within LIMS indefinitely. Data types and length of storage are retained in the Control of records SOP S-177-n.

i) Security

The company shall ensure that personal data is stored securely using modern software that is kept-up-to-date. Access to patient and personal data shall be limited to personnel

who need access and appropriate security should be in place to avoid unauthorised sharing of information. When personal data is deleted this should be done in a secure manner such that the data is irrecoverable. Appropriate back-up and disaster recovery solutions shall be in place.

The company have achieved the Cyber Esseentials Plus Certificate of Assurance. A copy of which is held on iPassport, M -1913-n.

j) Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the relevant user / information commissioners office.

k) Complaints about how we process your personal information

In the first instance, you should contact the Data Protection Officer – contact details above. Information about the rights of individuals under the Data Protection Act can be found online at:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

l) How to contact the Information Commissioner's Office (ICO)

You can contact the ICO at the following address and email:

Information Commissioner's Office

Wycliffe House

Water Lane,

Wilmslow SK9 5AF

www.ico.org.uk