ML Doctors GDPR Policy

Version number	1.1	**Document type**	Policy
Version date	25th March 2018	**Document ID number**	
Update Version date	22nd October 2019		
Version expiry	25th March 2020	**Document classification**	**PUBLIC**
Version status	Live document	**Uncontrolled if printed or downloaded**	

Amendment History

Date	Version	Author	Details of Amendment
14/3/17	1.0	S Densley	Initial Release
22/10/2019	1.1	D Raddings	Updated

ML Doctors operate as an Information Controller as defined under GDRP. We collect data via instructions from IPs, from various health authorities and related bodies and direct from the public in the form of consent forms. We store and use this data to instruct medical experts and provide treatment programs for clients as appropriate. We use a secure cloud-based system for managing appointments, records and reports and hold a GDPR complaint contract with the IT providers of that platform as they are data processors.

The ICO (Information Commissioners Office) have published a guide on how organisations should be approaching the implementation of General Data Protection Regulations. Below are the requirements of GDPR published by the ICO and how ML Doctors have approached these.

1. *Awareness You: should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.*

ML Doctors have published guidance documents for staff and ensured all staff and relevant 3rd parties have attended a “GDPR” awareness course held internally.

2. *Information you hold: You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.*

A data flow mapping exercise has taken place for all types of personal data we process or control. In addition to this we have Information Security Policies in line with our ISO27001 accreditation to ensure that date we hold is secure.

3. *Communicating privacy information: You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.*

ML have implemented their Information Security and Privacy Policies in line with ISO27001 and these can be viewed on our public web site and internal staff have been trained on the changes.

4. *Individuals' rights: You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.*

A defined process on how we obtain rights and transfer or delete personal information is now in place

5. *Subject access requests: You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.*

All staff have been trained on Data Subject Access Requests and a documented process for dealing with this has been published.

6. *Lawful basis for processing personal data: You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.*

ML Doctors have verified the lawfulness of processing and have a documented privacy policy in place which can be viewed on our website.

7. *Consent: You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.*

Consent is gathered where needed from data subjects and stored within our systems. We also have an appointed Caldicott Guardian who is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

8. *Children: You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.*

Children's information and consent is gathered from a parent or guardian. We also have an appointed Caldicott Guardian who is responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

9. *Data breaches: You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.*

Processes are in place to deal with any actual or attempted breach of personal data. These are individually logged including outcomes and lessons learned in line with ISO27001. Any such breaches are reviewed in monthly management meetings.

10. *Data Protection by Design and Data Protection Impact Assessments: You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party and work out how and when to implement them in your organisation.*

Data Protection Impact assessments are undertaken by ML Doctors as part of monthly ISO27001 and risk analysis meetings. These meetings are recorded, and outcomes published to relevant interested parties. A repeatable methodical, risk-based approach is used to identify and treat risks to personal data.

11. *Data Protection Officers: You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.*

ML have appointed a Data Protection Officer.

12. *International: If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.*

ML Doctors do not transfer or work outside of the EU. All our data and processing facilities are stored in the EEA.

Article 5

Article 5 (1) requires that personal data shall:

1(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, Fairless and transparency')

ML Doctors ensures to process the data in lawful, fair and transparent manner.

1(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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')

ML Doctors is to only use the data collected in the context of a Medical Legal Reporting Organisation and no other.

1(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

ML Doctors will only process the data relevant to its use within the context of a Medical Legal Reporting Organisation

1(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 ('accuracy')

ML Doctors will perform regular sampling on data to ensure accuracy. Any data identified as inaccurate will be verified and changed within the shortest time possible.

1(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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

Any data held by ML Doctors shall be retained for the period required by our regulators and/or UK legislations.

1(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 ('integrity and confidentiality').

ML Doctors will only process the data within the context of the organisation and/or through regulatory requirements.

Article 5(2)

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

ML Doctors ensures that it remains compliant with accountability while processing the data.

For any additional information please contact our Data Protection Officer (DPO)

Dan Raddings
IT Director
0161 839 3703