DATA SECURITY AND DATA RETENTION POLICY AND PROCEDURE

Data Retention

As a general principle, MCO Healthcare will not keep (or otherwise process) any personal data for longer than is necessary. If MCO Healthcare no longer requires the personal data once it has finished using it for the purposes for which it was obtained, it will delete the personal data unless it is required by law to retain the data for an additional period of time.

MCO Healthcare may have legitimate business reasons to retain the personal data for a longer period. This may include, for example, retaining personnel records in case a claim arises relating to personal injury caused by MCO Healthcare that does not become apparent until a future date. MCO Healthcare should consider the likelihood of this arising when it determines its retention periods - the extent to which medical treatment is provided by MCO healthcare will, for example, affect the likelihood of MCO Healthcare needing to rely on records at a later date.

MCO Healthcare may be required to retain personal data for a specified period of time to comply with legal or statutory requirements. These may include, for example, requirements imposed by HMRC in respect of financial documents, or guidance issued by the Home Office in respect of the retention of right to work documentation.

MCO Healthcare understands that claims may be made under a contract for 6 years from the date of termination of the contract, and that claims maybe made under a deed for a period of 12 years from the date of termination of the deed. MCO Healthcare may therefore consider keeping contracts and deeds and documents and correspondence relevant to those contracts and deeds for the duration of the contract or deed plus 6 and 12 years respectively.

MCO Healthcare will consider how long it needs to retain HR records. MCO Healthcare may choose to separate its HR records into different categories of personal data (for example, health and medical information, holiday and absence records, next of kin information, emergency contact details, financial information) and specify different retention periods foreach category of personal data. MCO Healthcare recognises that determining separate retention periods for each element of personal data may be more likely to comply with GDPR.

MCO Healthcare may decide, however, that separating its HR records into different elements is not practical, and that it can determine a sensible period of time for which to keep the HR records in their entirety. The period of time that is appropriate may depend on the likelihood of a claim arising in respect of that employee in the future. If, for example, MCO Healthcare is concerned that an employee may suffer personal injury as a result of its employment with MCO Healthcare, MCO Healthcare may choose to retain its HR records for a significant period of time. If any such claim is unlikely, MCO Healthcare may choose to retain its files for 6 or 12 years (depending on whether the arrangement entered into

between MCO Healthcare and the employee is a contract or a deed).

MCO Healthcare will consider the following advice and guidelines when deciding for how long to retain HR data. MCO Healthcare acknowledges that the suggested retention periods below are based on guidance within relevant legislation:

• Immigration checks - two years after the termination of employment
• PAYE records- at least three years after the end of the tax year to which they relate
• Payroll and wage records for companies - six years from the financial year-end in which payments were made
• Records in relation to hours worked and payments made to workers - three years beginning with the day on which the pay reference period immediately following that to which they relate ends.

Records required by the Working Time Regulations:

• Working time opt out - two years from the date on which they were entered into
• Compliance records - two years after the relevant period
• Maternity records - three years after the end of the tax year in which the maternity pay period ends
• Accident records - at least three years from the date the report was made, or potentially longer if deemed appropriate given the possibility of ongoing relevance of the records.

MCO Healthcare will consider for how long it is required to keep records relating to Clients. In doing so, MCO Healthcare will consider the data retention guidelines provided by the NHS, if applicable. If the NHS guidelines do not apply to MCO Healthcare, MCO Healthcare will determine an appropriate retention policy for Client personal data. MCO Healthcare may choose to retain personal data for at least 6 years from the end of the provision of services to the Client, in case a claim arises in respect of the services provided.

Irrespective of the retention periods chosen by MCO Healthcare, MCO Healthcare will ensure that all personal data is kept properly secure and protected for the period in which it is held by MCO Healthcare. This applies in particular to special categories of data.

MCO Healthcare will record all decisions taken in respect of the retention of personal data. MCO Healthcare recognises that if the ICO investigates the policies and procedures at MCO Healthcare, a written record of the logic and reasoning behind the retention periods adopted by MCO Healthcare will assist the position of MCO Healthcare.

MCO Healthcare will implement processes for effectively destroying and/or deleting personal data at the end of the relevant retention period. MCO Healthcare will consider whether personal data stored on computers, including in emails, is automatically backed up and how to achieve deletion of those backups or ensure that the archived personal data is automatically deleted after a certain period of time. MCO Healthcare will consider

circulating guidance internally to encourage staff to regularly delete their emails. MCO Healthcare will introduce policies relating to the destruction of hard copies of documents, including by placing the documents in confidential waste bins or shredding them.

Data Security

MCO Healthcare will take steps to ensure that the personal data it processes is secure, including by protecting the personal data against unauthorised or unlawful processing and against accidental loss, destruction or damage.

MCO Healthcare understands that the following types of organisation must comply with Data Security and Protection :

- Organisations contracted to provide services under the NHS Standard Contract
- Clinical Commissioning Groups
- General Practices that are contracted to provide primary care essential services

Local authorities should comply with data protection where they provide adult social care or public health and other services that receive services and data from NHS Digital, or are involved in data sharing across health and care where they process confidential personal data of Clients who access health and adult social care services.

Social care providers who provide care through the NHS Standard Contract should comply with the toolkit. It is also recommended that social care providers who do not provide care through the NHS Standard Contract consider compliance with data protection as this will help to demonstrate compliance with the data security standards and GDPR.

MCO Healthcare will implement and embed the use of policies and procedures to ensure that personal data is kept secure. MCO Healthcare will bear in mind the following principles when deciding how to ensure that personal data is kept secure:

Confidentiality- ensuring that personal data is accessible only on a need to know basis

Integrity - ensuring that there are processes and controls in place to make sure personal data is accurate and complete

Availability - ensuring that personal data is accessible when it is needed for business purposes of MCO Healthcare

Resilience - ensuring that personal data is able to withstand and recover from threats For paper documents, these will include, where possible:
Keeping the personal data in a locked filing cabinet or locked drawer when it is not in use.

Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them.
Redacting personal data from documents where possible.
Ensuring that documents containing personal data are placed in confidential waste bins or shredded at the end of the relevant retention period.
Minimising the transfer of personal data from outside of business premises and, where such transfer cannot be avoided, ensuring that the paper documents continue to be kept confidential and secure.

For electronic documents, the measures taken by MCO Healthcare will include, where possible: Password protection or, where possible, encryption.
Ensuring that documents containing personal data are accessible only by those who need to know/review the documents and the personal data contained within them.

Ensuring ongoing confidentiality, integrity and reliability of systems used online to process personal data (this may require a review of IT systems and software currently used by MCO Healthcare)The ability to quickly restore the availability of and access to personal data in the event of a technical incident (this may require a review of IT systems and software currently used by MCO Healthcare)Taking care when transferring documents to a third party, ensuring that the transfer is secure and the documents are sent to the correct recipient MCO Healthcare will ensure that all business phones, computers, laptops and tablets are password protected. MCO Healthcare will encourage staff to avoid storing personal data on portable media such as USB devices. If the use of portable media cannot be avoided, MCO Healthcare will ensure that the devices it uses are encrypted or password protected and that each document on the device is encrypted or password protected.

MCO Healthcare will implement guidance relating to the use of business phones and messaging apps. MCO Healthcare understands that all personal data sent via business phones, computers, laptops and tablets may be captured by GDPR, depending on the content and context of the message. As a general rule, MCO Healthcare will ensure that staff members only send personal data by text or another messaging service if they are comfortable that the content of the messages may be captured by GDPR and may be provided pursuant to a Subject Access Request (staff should refer to the Subject Access Requests Policy and Procedure at MCO Healthcare for further details).

MCO Healthcare will ensure that all staff are aware of the importance of keeping personal data secure and not disclosing it on purpose or accidentally to anybody who should not have access to the information. MCO Healthcare will provide training to staff if necessary. MCO Healthcare will consider, in particular, the likelihood that personal data, including special categories of data, will be removed from the premises of MCO Healthcare and taken to, for example, Clients' homes and residences. MCO Healthcare will ensure that all staff understand the importance of maintaining the confidentiality of personal data away from the premises of MCO Healthcare and take care to ensure that the personal data is not left anywhere it could be viewed by a person who should not have access to that personal data.

MCO Healthcare will adopt policies and procedures in respect of recognising, resolving and reporting security incidents including breaches of GDPR. MCO Healthcare understands that it may need to report breaches to the ICO and to affected Data Subjects. MCO Healthcare will adopt processes to regularly test, assess and evaluate the security measures it has in place for all types of personal data. Privacy by Design MCO Healthcare will take into account the GDPR requirements around privacy by design, particularly in terms of data security.

MCO Healthcare understands that privacy by design is an approach set out in GDPR that promotes compliance with privacy and data protection from the beginning of a project. MCO Healthcare will ensure that data protection and GDPR compliance is always at the forefront of the services it provides, and that it will not be treated as an afterthought.

MCO Healthcare will comply with privacy by design requirements by, for example: Identifying potential data protection and security issues at an early stage in any projector process and addressing those issues early on; and Increasing awareness of privacy and data protection across MCO Healthcare, including in terms of updated policies and procedures adopted by MCO Healthcare. MCO Healthcare will conduct Privacy Impact Assessments to identify and reduce the privacy and security risks of any project or processing carried out by MCO Healthcare. A template Privacy Impact Assessment is available within the Privacy Impact Assessment Policy and Procedure at MCO Healthcare Section.

Procedure

MCO Healthcare will consider data retention and data security issues and concerns at the beginning of any project (whether the project is the introduction of a new IT system, a new way of working, the processing of a new type of personal data or anything else that may affect the processing activities at MCO Healthcare). MCO Healthcare appreciates that this is key for complying with the privacy by design requirements in GDPR.

MCO Healthcare will review the periods for which it retains all the personal data that it processes. MCO Healthcare will, if necessary, adopt new policies and procedures in respect of data retention and will circulate those policies and procedures to all staff.

MCO Healthcare will consider providing training to staff in respect of data retention. MCO Healthcare will review the security measures currently in place in respect of all the personal data it processes.

MCO Healthcare will document the decisions it takes, and the logic and reasoning behind those decisions, in respect of both data retention and data security. MCO Healthcare will keep a record of all policies and procedures it implements to demonstrate its compliance with GDPR.

Last updated 13/10/2022