Policy Title	**Data Protection and Medical Records Management**
Policy Number	EDOOP.009
Purpose	To ensure all information we hold is recorded, kept securely and managed in accordance with current legislation, best practice and guidance. To ensure a business continuity plan is in place should data be lost or become inaccessible.
Author	Dr Aaron Pennell – Clinical Director Dr Anup Mathew – Clinical Director
Responsible officer/s	Dr Aaron Pennell - Clinical Director
For use by	All Clinical Staff, Executive Management Team
This policy complies with or has been guided by	Data Protection Act 1998. Access to Health Records Act 1990 The Access to Medical Reports Act 1988 Human Rights Act 1998 Freedom of Information Act 2000 Regulation 20 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2010
CQC outcome compliant	Outcome 21
This document supersedes	EDOOP/009/01/12/V1
Approved and ratified by	Executive Management Group
Implementation date	1st January 2012
Review date	1st February 2017
Version and Document Control	Version 2 - reviewed and edited February 2015

Equal Opportunities, Health and Safety, Employment conduct and Professional Liabilities Assessment:

EDMS has ensured given every reasonable means and with the information available at this time that this policy will not discriminate either directly or indirectly in any way against employees, patients or customers on the grounds of race, religion, colour, age, gender or sexual orientation, disability, marital status or culture. EDMS has assessed this policy in terms of current health and safety guidance and has ensured that where requirements have been stipulated these are met. EDMS has ensured that it holds appropriate insurance for this policy to be fully endorsed. EDMS has assessed this policy for any impact it may have on corporate or individual professional requirements and conduct and has ensured any such impact meets with the approval of any professional bodies it may encounter. This policy can be made available in Braille or voice recording and can be translated into other languages

1. Executive summary

EDMS creates, retains and where indicated releases information regarding employees, patients and contracts. It is essential that the ways these activities are managed meets current legislation and are coordinated in a robust framework. In addition the management of medical records requires special attention in terms of high levels of patient confidentiality, guidance on the sharing of patient information with other health care providers and access to medical records by the patient.

2. Terminology (if needed)

- **Caldicott Guardian** – A senior person within the organisation who has overall responsibility for the secure handling or clinical records and who had authority and training to decide when and how information should be shared. The Caldicott Guardian should ensure clinical records are maintained, stored and shared following 6 principles:
    - **Principle 1** – Justify the purpose(s) for using confidential information
    - **Principle 2** – Only use it when absolutely necessary
    - **Principle 3** – Use the minimum that is required
    - **Principle 4** – Access should be on a strict need-to-know basis
    - **Principle 5** – Everyone must understand his or her responsibilities
    - **Principle 6** – Understand and comply with the law

3. General Policy regarding all data.

The Data Protection Act 1998 concerns personal privacy and regulates how information about living individuals may be collected, used, retained and disclosed. All processing of personal data must be notified to the Information Commissioner.

The new Act applies to all personal data whether it is in paper or electronic format. Individuals are entitled to see all information kept about them. Members of staff should be open with individuals about any information held about them. Staff should also be careful about passing any personal information on to third parties.

EDMS holds information regarding its members of staff, contacts and those we hold contracts with and finally information about service users, in terms of patient report forms/records of those we assess and treat.

This policy gives a brief and simple outline of the responsibilities of staff under the Data Protection Act 1998 and the Health and Social Care Act 2008

There are 8 principles of data protection:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purpose(s) and shall not be further processed in any manner incompatible with that purpose(s).
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area (without the individual's express consent) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Consequently, there are 8 fundamental measures to achieve compliance:

Principle 1
No personal data should be created or held unless the individual has given his/her consent. Where sensitive data is concerned specific consent must be obtained - the individual must be informed that this type of personal data is being held, told the reason for it and must then agree. Photographs are classified as sensitive data because they may reveal information about the subject's race and ethnicity. Permission should always be obtained to keep or use a photograph of an individual.

Principle 2
Do not use data obtained for one purpose for a different purpose. For example, a list of members of staff or course students should not be used for commercial mail shots.

Principle 3
Do not collect information about individuals which is not absolutely necessary. Do not ask questions seeking data without ensuring that the question is strictly relevant. If excessive or superfluous personal data is acquired it should be deleted or destroyed immediately.

Principle 4
If data is retained it must be reviewed and if necessary amended or updated. No data should be kept unless it is reasonable to assume that it is accurate.

Principle 5
Regular and systematic reviews of files (both paper and electronic) containing personal data should take place to ensure that information is not retained for longer than is necessary.

Principle 6
The rights of individuals in respect of their data should always be considered. Consent should be obtained if personal data is to be generated or retained for any purpose. Data subjects are legally entitled to know what information is being held about them. It is also important that no personal data is disclosed to anyone, either inside or outside AMS, unless strictly necessary or unless the consent of the data subject has been obtained.

Principle 7
Staff must ensure that any personal data is kept in a secure place - in lockable filing cabinets or in rooms which can be locked when unoccupied. They must also seek to prevent unauthorised access to any computers in which personal data is stored.

Principle 8
No personal data should be transferred, even for a legitimate purpose, outside of the European Economic Area (EEA) except with the specific consent of the data subject. This is particularly important when considering the global publication of personal information via the World Wide Web.

Rights of the Individual:

Under the Data Protection Act 1998 individuals have the right to inspect all personal information held about them. This includes the contents of course student files, staff files, application forms, and lists of members of staff who occasionally work for us.

Patient records are treated slightly differently given the sensitive nature of their content.

a) With regard to personal data EDMS shall ensure that such data:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for that purpose.

- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data

b) The nominated Data Controller for EDMS is Dr Anup Mathew, Clinical Director.

c) With regard to the security of personal data, all staff should ensure that:

- Any personal data that they hold is kept securely in a locked drawer, filing cabinet or safe
- If computerised data is held then it should be encoded, encrypted or password protected on the computer, network system or external hard drive. Where external devices are used they should be locked away when not in use or under direct control of an authorised individual.
- Personal data MUST NOT be placed on memory sticks, personal computers or stored electronically on virtual servers.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

d) Release of information, unless authorised or failure to store and handle information outside of the above guidance may lead to disciplinary action being taken including reporting to a regulatory body.

e) Access to data must be via the data controller who will decide on the extent of access required and record that data has been accessed.

General Policy – Medical Records

a) Medical records in the form of patient report forms and other continuation sheets will be kept in a secure metal cabinet that will be locked at all times. Access to these records will be via the Clinical director only or nominated director in his absence. The exception being patients with active episodes where the records will be stored securely but all staff involved in their care, treatment or support will have where appropriate access to refer to and contribute to the record until the episode is closed

b) Only such information as is absolutely necessary shall be held as records. Any data considered unnecessary shall be disposed of securely by means of disk destruction, paper shredding or wiping securely of any electronic media.

c) Records about care, treatment and support of people who use services must be updated as soon as is practical following delivery of that care, treatment or support. Any verbal communications about care, treatment or support must also be recorded within their personal records as soon as is practical. New episodes must be linked to old episodes so a complete single record is held

d) Records about care, treatment and support must be factual and accurate and maintain the dignity and confidentiality of the people who use the service. They are used to plan appropriate care, treatment and support to ensure their rights and best interests are protected and their needs are met.

e) A review of all data stored shall be made monthly by the office manager. Any material thought to be unnecessary shall be discussed with a director who will authorise destruction in accordance with the Data Protection Act and the Department of Health's Records Management: NHS code of practice (part 2)

f) Patients who wish to access their medical records may so by making their request in writing to the medical director. Service users will be contacted within 7 days of that letter to make an appointment to view their medical records. Where copies are requested a fee of £30.00 per record is chargeable.

g) All staff on joining EDMS will have issued a guidance document on data protection and patient confidentiality. Once read and understood this shall be signed by the individual and kept with their personal file. Aspects of data protection and confidentiality are covered on the induction and mandatory training course

Management of Medical Records Operational Aspects:

a) A Clinical Record Form (CRF) must be completed for every patient episode. The forms are available in every critical care pack and minor injuries pack as well as having stocks in the documentation boxes.

b) The top (white) copy is kept by EDMS and the bottom (yellow) copy given to the patient / ambulance crew etc

c) Completed medical records must be stored in the secure documentation box at events etc. Where the documentation box is not used, completed CRF's must be placed in the document wallet and returned to the office for storage in the clinical records safe.

d) On NO account must CRF's be posted, scanned, photographed or left in vehicles etc.

e) Any missing CRF's must be reported to the clinical director as a matter of urgency.

Legal requirements to hold records for a minimum time period

The Health and Social Care Act 2008 requires specific types of records to be held for a minimum period of time only after which can they legally be destroyed.

- Risk assessments; retain the latest risk assessment until a new one replaces it
- Purchasing excluding medical devices and medical equipment; 18 months
- General operating policies and procedures; retain the current version and previous version for three years
- Any incidents, events or occurrences that require notification to the Care Quality Commission; three years
- Use of restraint or the deprivation of liberty; three years
- Detention; three years
- Maintenance of the premises; three years
- Maintenance of equipment; three years
- Electrical testing; three years
- Fire and water safety; three years
- Medical gas safety, storage and transport; three years
- Money or valuables deposited for safe keeping; three years
- Staff employment; three years following date of last entry
- Duty rosters; four years after the year to which they relate
- Purchasing of medical devices and medical equipment; 11 years
- Final annual accounts; 30 years.

End