Confidentiality and the General Data Protection Regulation (GDPR)

All doctors must follow GMC guidance on Confidentiality when using or sharing patient information: https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality The GDPR does not make any fundamental changes to the this guidance.

It is unlikely that salaried doctors will be 'data controllers' for the purposes of the GDPR. A data controller is a person or organisation that decides why and how personal data are processed.

All organisations must have data protection policies and procedures in place in order to meet their legal obligations under GDPR, for example, managing subject access requests, reporting data breaches and staff training. Salaried doctors must follow their local policies and procedures.

Many breaches of confidentiality occur inadvertently. Some practical tips which all health and care staff can use to help ensure that confidential information is protected at all times include:

- Don't share password logins or smartcards and don't leave terminals unattended when logged in
- Don't leave paper records unsupervised where they might be accessed inappropriately
- Don't download confidential information onto unencrypted portable devices such as USB sticks
- Know who to talk to in your organisation if you are unsure, for example, your Caldicott Guardian or an experienced colleague
- Avoid discussing cases in public places if the patient can be identified

Dame Fiona Caldicott, the National Data Guardian for Health and Social Care has established seven key principles for health and care staff to guide how they use and share confidential information:

Principle 1 – Justify the purpose(s) for using confidential information
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

Principle 2 – Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

Principle 3 – Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.
Principle 4 – Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

Principle 5 – Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data - both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

Principle 6 – Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be 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 within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.