The use of confidential patient data in healthcare is and always has been commonplace and essential in order to ‘get the job done’. Without data collection and use, healthcare would not be possible. Data use is so commonplace in healthcare that it is easy to forget just how sensitive some of the data is. Doctors and other healthcare providers often forget about the need to ensure the safe storage and handling of clinical data.

Medical records are generally considered by members of the public, by patients, to be of the most sensitive type of data, that should not be disclosed to others, save in very carefully controlled and secure circumstances, and only when absolutely necessary. Where data is lost, stolen or mishandled, patients may lose significant confidence in their doctor and healthcare providers. The press too may well focus on any data loss or misuse in a politicizing and sensational way, causing doctors reputational damage. It is often the case that doctors and healthcare providers only properly review their policies after things have gone wrong. The GMC and the Data Commissioner, or even the police, may become involved, and a doctor or healthcare provider may have a lot of explaining to do.

Compliance with GDPR pursuant to Data Protection Act 2018 (formerly the Data Protection Act 1984, the Data Protection Act 1988, the Data Protection Act 2003) is essential. Breaches can lead to significant fines or regulatory interventions, and
in some instances could be career ending.

Doctors who are in private practice will need to register with the Information Commissioner as a data controller, as will certain doctors who manage an NHS services under contract or otherwise – such as GPs. The annual fee is a modest £35 and the commissioner must be informed (by way of completion of a data protection form). Visit the information Commissioner’s Office (ICO) Website for more details. See also the ICO web page dedicated to patients, which provides details of how they may obtain information about themselves. For guidance on GDPR, see a further ICO webpage: GDPR Compliance

It is essential that doctors and healthcare organisations have in place an up to date and regularly reviewed data protection policy. One which details the type of data that is held, the nature of any data examination, the people who will have permitted access, how the data will be kept secure, and how

ipads are usually encrypted and can be remotely wiped if lost or stolen. With a password set up, the drive can be set to automatically wipe if an incorrect password is entered too many times. Laptops and desktop computers generally do not come with encryption, but additional software can be purchased that can undertake the task on the fly, seamlessly. Encrypted drives can also be purchases, as can encrypted USB drives.

Paperwork must be stored in a locked cupboard and good records should be kept of its location, the period it is to be retained, who has access to it, and the locations in which the paperwork can be scrutinised or analysed.

In many instances, the nature of a clinicians work may be such
that they will need to take confidential material out of work. Perhaps to a meeting at another location, or for working on at home. Any policy should reflect this, and papers and computer data will need to be locked away when not in use. Many healthcare providers insist that no clinical data is taken off the premises. This is not always realistic or achievable, particularly with commissioning and independent contractors coming and going to provide certain services.

The nature of the data analysis needs to be carefully considered, and any output that is used publicly must be anonymised, and might require permission for disclosure in certain forms.

The GMC has also created a useful set of guidelines, which focus on healthcare and the protection and storage of data. The guidelines also make reference to Department of Health guidelines for the safe handling of medical records. Download from the GMC in PDF format the latest guidelines: Confidentiality. See also the GMC’s supplementary advice on when to disclose confidential information.

Doctors Defence Service can advise doctors and healthcare providers on data protection policies and the Data Protection Acts. Where things have gone wrong, Doctors Defence Service can assist doctors in putting things right, crafting an apology, liaising with the Data Commissioner, the police or GMC. Call us on 0800 10 88 739 for further details of how we might assist you, or use our Contact Form.