Medical Podcasts In English For Non-Native Speakers

S1 E3 GDPR and doctors.

Most people will have heard of the General Data Protection Regulation or GDPR which came into effect in May 2018, if only because of the pop-ups requesting permissions or in the case of certain non-EU websites, being refused access altogether.

If you are still using paper records or are outside of the EU, this too affects you as all data are covered by articles 2 and 3 of the GDPR.

For doctors, the essential concepts to understand about data processing or actions on information that can identify their patient are three:

1. The first one is "**Data controller"**: Person who decides what data is collected, how this data is collected and for which purpose. As a doctor, you or your institution can be a data controller.
2. The second concept is to understand what or who is a "**Data processor"**: It is a person or service who processes the data under the instructions of the controller and as a doctor using digital technology this can be the software you are buying to store the data.
3. The final concept is the "**Data subject"**: This is the patient or identifiable person.

Article 5 of the GDPR covers data processing, and as a doctor/data controller, you need to be aware that the data you collect should be:

1. **Lawful, fair and transparent**.
2. **Limited to purpose** – you need to be recording data with a specific, limited and explicit purpose.
3. **Minimised** – irrelevant data should not be recorded.
4. **Accurate** – doctors are used to making notes on treatment changes, for example, and we are all aware of the legal consequences of not keeping legible notes.
5. **Limited storage** – this refers to not keeping the data for longer than required. Health is probably one of the few exceptions where you can argue that the data should be stored for the entire life of a person to give the best care.
6. **Integrity and confidentiality**. This refers to the fact that the data must be protected appropriately through technical and organisational means. You need to consider not only loss and damage (accidental or other) but also that it is *not accessed inappropriately by different members of staff*. This is a core question when being presented with a new medical

application or technology for your practice. Larger institutions such as hospitals will have an information security officer, but *if you practise in a smaller setting, this responsibility will be yours.*

Finally, to process any data, you need to be sure that there are legal grounds for processing the data you have collected. For doctors, the concepts are familiar:

1. **Consent** has been given.
2. It is necessary for a **contract** to be carried out and specifically, in the health care setting, this includes an agreement to medical treatment either implicitly or explicitly.
3. You are complying with a **legal obligation**.
4. You are protecting the **vital interests** of a patient.
5. You are carrying out a task in the **public interest** or in your capacity as an **official authority.**
6. There exists a **legitimate interest** for processing.

Although this is quite a dry topic, for doctors it is actually just formalising our usual practise and therefore probably easier than for us than for most people to understand what the GDPR is about.

The important points are to understand and decide if you are a data controller or data processor and then it is easier to understand the responsibilities linked to those roles.

S1 E3 GDPR and doctors.

1) *At your current workplace are you the data controller or/and data processor?*

2) *Review 3 sets of patient notes and think about whether you are GDPR compliant. Hint: Refer to the check-list above.*

3) *Identify your DPO and make sure you are on a mailing list for any data protection updates.*

4) *Check your own health apps or systems used by your personal doctor. Are they GDPR compliant?*