FMiL
Institut de Formació
Mèdica i Lideratge

Medical Podcasts In English For Non-Native Speakers

S1 E4 What is the difference between pseudonymisation and anonymisation?

Sensitive data, as health data is, get more privacy protection, and Article 9 of the GDPR we explained about last week covers this specifically. Safeguards used include pseudonymisation, anonymisation and encryption

Pseudonymisation:

- This is removing identifying fields such as name, date of birth and address but in health needs to go even further. A diagnosis of a specific disease and treating hospital plus gender may be enough to identify the patient.
- With big data and large amounts of patients, it becomes harder to identify individuals, but even there it is important to think about unusual characteristics which may make the patient stand out.
- Some doctors have fallen foul to this on twitter when making what they thought were generic comments about a type of patient they may have seen during a specific shift.
- However, at the same time you still have to have the correct data to treat your patient. This means that you need additional information in order to access all the information about your specific patient.

Anonymisation:

- This means that you strip away all the identifying aspects from the data and can no longer identify the patient. This is a valid technique for research. You can no longer identify the person even if you have the additional information.
- It is very hard to anonymise medical data and there is a chilling report for all those with any level of data protection responsibility. Supposedly anonymised health data sets were not so anonymous once compared to local newspaper reports. 43% of the individuals were identified.

Encryption:

- This encoding of the data is very much more a technical aspect.
- Most doctors would find it hard to know what questions to ask and then interpret the answers. However, thinking of specific clinical contexts may make the technical team think about uses and deviations which they had not come across.

In general, observing good medical practice will set you on the right road, but the questions come when you or your hospital or practise are looking to change your EHR (electronic health records) system. Or even to check if the system you are currently using is compliant.

Most clinicians without any programming or technical knowledge would find it hard to ask programmers specific questions and then understand the answers. However, technicians don't have the situation-specific understanding of how this data will be used and going through a typical consultation together step by step can help uncover moments when there may be data compliance issues.

Data protection by default

In other words, only the sensitive data needed for the specific process can be processed. An example of this would be:

- How do you lock the screen temporarily while examining a patient when family members may be present?
- How do you deal with multiple doctors using the same computer?
- How are blood results transferred between the laboratory and your EHR?
- Are emails encrypted if you have to do a referral to a colleague?

Data protection officer.

If you are part of a larger institution there will be an appointed data protection officer and your obligation is to contact them rather than sort it out yourself. However, if you have seen something you do need to report it? You can't just pretend you didn't see it as you will have created an electronic trail which can be audited.

S1 E4 What is the difference between pseudonymisation and anonymisation?

1) *What / who is the data processor that is being used by your current EHR?*

2) *As this is sensitive data, how is it:*
    a) *Pseudonymised?*
    b) *Encrypted?*

3) *How is it complying with data protection by design and default?*

Hint: A quick email to your DPO will probably give you the answers to all of these questions.