INFORMATION GOVERNANCE BRIEFING

Information Governance - The Portugal Hospital Case

The General Data Protection Regulation (GDPR) was drafted by the European Data Protection Board and implemented the same across all the EU states. This means that many of the legal judgements based on it can be used as a benchmark in other EU countries, as it would be expected that the law will be interpreted by judges in broadly the same way.

The first significant fine under GDPR was issued by the Portugal Data Protection regulator to a hospital for €400,000 in October 2018, and the ruling has significant relevance to our healthcare setting.

There was an investigation at the hospital which revealed that the hospital's staff; psychologists, dietitians, and other professionals, had access to patient data through inaccurate access role profiles. The profile management system appeared deficient – the hospital had 985 registered doctor profiles while only having 296 doctors. Moreover, all doctors had unrestricted access to all patient files, regardless of the doctor's speciality. It was concluded that the hospital did not put in place appropriate technical and organisational measures to protect patient data as required by GDPR.

Some facts considered proven by the investigation:

- Nine IT technical employees had the level of access reserved for the medical group, which resulted in the possibility of such employees accessing the clinical records of all hospital users.
- Existence of access credentials which allowed any doctor, regardless of his/her specialty, to access at any time the data of all the patients at the hospital. This was considered as violating the principle of "need to know" and the principle of "minimisation of data – both Caldicott Principles in the UK.
- There were 985 users associated with the profile "doctor," but in the official hospital human resources charts there are only 296 doctors in that hospital.

So, what can we learn in respect of our clinical systems and the way we manage them?

- First, practices must document and manage the access profiles of their users in the clinical system they use. The N3i RA Team can help with this, but it is an ongoing task for the practice to manage the access rights and users it allocates them to.
- A user must never be given an access profile that they do not require or does not describe their function. A suitable role should exist for all users, please ask if there is not one that accurately reflects the user's situation. This will include non-clinical staff.

Finally, the key concepts of approved access rights and Position Based Access Control, enforced through NHS Smartcards exist in systems for a reason, but they only work when they are implemented, maintained and used correctly.