Data Protection and Audit – Dr Claire Collins (October Forum 2019)

Claire Collins looks at regulatory issues relating to audit and where patient consent may come into play.

GDPR is the EU's new General Data Protection Regulation (EU) 2016/679. It came into force across all of Europe in May 2018. It replaced the EU's previous Data Protection Directive (95/46/EC). GDPR governs the collection, use and storage of all personal data of living individuals. The Data Protection Act 2018 is the Irish legislation that gives effect to certain aspects of the EU's GDPR in Ireland and repeals, for the most part, the previous Data Protection Acts 1998 and 2013. If you collect, use or store personal data in digital, manual, handwritten or any type of record, then GDPR affects you.

Given these changes, the Medical Council has published advice in relation to conducting your audit:

- All registered medical practitioners are legally required to maintain their professional competence. This means that as well as undertaking 50 CPD credits, they also need to complete and record one clinical/practice audit annually. Employers are legally required to facilitate the maintenance of professional competence of registered medical practitioners.
- During the clinical/practice audit process, health data is processed. Even if the health data is anonymised shortly after it is retrieved from patient records for the purpose of clinical/practice audit, that retrieval process in itself amounts to processing. Health data is defined under the GDPR as special category data. Such data can be processed in situations where it is necessary to do so for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of healthcare (Article 9(2) of the GDPR).
- Medical practitioners can lawfully process special category data for the purposes of clinical/practice audit. However, in doing so, they must ensure that they adopt suitable and specific measures to safeguard the fundamental rights and freedoms of the data subjects concerned.
- Consent is just one of the legal bases upon which data controllers can rely in order to lawfully process special category data.
- Given the high threshold for consent and the fact that it can be withdrawn at any time, and in circumstances where there is another legal basis available to the practitioner to lawfully process a patient's special category data (Part 11 of the Medical Practitioners Act 2007), it is not recommended to rely on consent as the legal basis for the processing of special category personal data for the purpose of clinical/practice audit. This means that medical practitioners (and their employers) are not required to seek consent before processing special category data for the purposes of undertaking a clinical/practice audit.
- However medical practitioners (and employers) should ensure that they are compliant with the transparency obligation in the GDPR Article 5(1)(a) by ensuring that comprehensive privacy notices are provided to their patients. Further details on what privacy notices constitute can be found in the GDPR.
- Each medical practitioner is either a data controller in their own right, or is employed by a data controller (for example a hospital). Every data controller is responsible for ensuring that they are compliant with the GDPR. The Medical Council can only give guidance in this regard. In light of this, medical practitioners should liaise with their data protection officer or seek their own legal advice on this issue.
- Further information and resources on data protection is available at www.medicalcouncil.ie/FOI-Data-Protection/

Public health lawful basis

The National Office of Clinical Audit (NOCA) has advised that national clinical audit should not rely on consent as the lawful basis but instead apply the public health lawful basis of Articles 6(1)(e) and 9(2)(h) of the GDPR. The collection of data, validation of data, and review of outliers for national clinical audit does not require consent. However, patients should be informed that their data may be used as part of a national clinical audit.

Adopting suitable and specific measures

In summary, during a clinical/practice audit, health data is processed and the process of data retrieval/extraction from the patient record in itself amounts to processing. However, such data can be processed in situations where is it necessary to do so for reasons of public interest in the area of public health, such as ensuring high standards of quality and safety of healthcare (Article 9(2) of the GDPR).

Hence, you can lawfully process special category data for the purposes of clinical/practice audit; however, you must ensure that you adopt suitable and specific measures to safeguard the fundamental rights and freedoms of the data subjects concerned.

You, therefore, are not required to seek consent before processing special category data for the purposes of undertaking a clinical/practice audit once you ensure that you are compliant with the transparency obligation in the GDPR Article 5(1)(a) by ensuring that comprehensive privacy notices are provided to your patients.

It is important to inform patients that the practice may use data for internal audit. This can be included in a patient information leaflet, in a privacy statement, on patient registration forms or on the practice website. It is not acceptable for external research staff to trawl through individual patient records without informed patient consent. It is also not acceptable to release the contact details of patients to researchers without informed patient consent. Identifiable data should not be used – only anonymous data should be extracted/compiled for the audit.

Audit is not research however, and different and additional rules apply. You cannot personally use your patients' health data or share their health data with a third party individual or organisation, for research purposes, without the patient's explicit consent, unless the research has obtained a consent declaration under the new Health Research Regulations 2018.