Data Protection and confidentiality in GP surgeries

Ash Jilani
Head of Primary Care
01622 776402
ashjilani@brachers.co.uk

In August 2016, Regal Chambers, a GP surgery in Hitchin, Hertfordshire was fined £40,000 by the Information Commissioner for revealing confidential information about one of their patients to her estranged ex-partner, despite express warnings given by the woman to practice staff to protect her details.

The woman's ex-partner formally requested the medical records of their son under the Data Protection Act (known as a subject access request). The Practice did not have an adequate written procedure or system for handling these requests. In the absence of proper supervision or guidance, the person handling the request went ahead and sent 62 pages of the son's medical records to his father, which contained the woman's personal contact details (as well as those of her wider family).

An ICO investigation found that the GP practice had insufficient systems in place to guard against releasing unauthorised personal data to people who were not entitled to see it. This was a breach of the seventh principle of the Data Protection Act 1998, namely, having in place appropriate technical and organisation measures to prevent the unauthorised or unlawful processing of personal data.

This case highlights the importance of providing staff with proper training and guidance and having appropriate systems to safeguard against unauthorised disclosures.

Whilst most practices will have some sort of system in place, with the increasing workload and pressure on practices, sometimes basic principles can easily be overlooked.

It is important to note that anyone who processes personal information must comply with eight principles of the Data Protection Act, which make sure that personal information is:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- not kept for longer than is necessary;
- processed in line with your rights;
- secure against unlawful processing, loss or destruction; and
- not transferred to other countries without adequate protection.

Given the sensitive and personal nature of the information GPs hold about their patients, the ICO is naturally concerned with ensuring maximum compliance. Since February 2015, the ICO has been able to carry out compulsory audits to assess data protection by organisations including GP practices.

So what can you do to guard against such a situation arising in your practice? We list a few pointers below:

- Every practice should appoint someone who is responsible for supervising data security procedures and handling requests to access records;
- Formal, written procedures and clear instructions should be provided to staff to follow when responding to such requests;
- Practices must make sure to identify what information can be disclosed and what

Data Protection and confidentiality in GP surgeries

information must be with held

- Information concerning people other than the person making the request must be redacted where possible or otherwise, consent must be sought;
- GPs should provide support and guidance to practice staff as much as possible during the process; and
- Staff should be provided with comprehensive training and regular training on data protection compliance.

Our commercial team can assist your practice with data protection compliance including advising on policies and procedures; responding to requests for disclosure of information and providing tailored staff training on data protection issues.

Brachers
With you all the way

www.brachers.co.uk
01622 690691

Head Office
Somerfield House
59 London Road
Maidstone
Kent ME16 8JH

@brachersllp

Brachers LLP