BMA

GPs as Data Controllers

What is a data controller?

– Under the Data Protection Act 1998 (DPA), the data controller is the person (or organisation) that 'determines the purposes for which and the manner in which any personal data are to be processed'.[1] In other words, the data controller has overall control of the data and decides how and why data are to be processed.

– GP practices are data controllers for the information they hold about their patients. Most practices will have 'data processing'[2] arrangements with third parties, for example IT system suppliers carry out a wide range of clinical and administrative processes within the practice, but it is the data controller[3] who retains responsibility for compliance under the Act.

– The data processor can only act in response to an instruction from the data controller. Any change in the processing arrangements or significant decisions about the data must be made, or agreed with, by the data controller.

– The data controller has a legal responsibility to control the way in which a data processor processes the data. Contractual arrangements must set out these responsibilities and should include, for example, assurances that the data processor has adequate security measures in place. This would be particularly important should a data breach occur.

– As data controllers, GPs retain responsibilities for handling all requests for access to the data, for example, subject access requests made by patients or requests from third parties such as insurance companies and solicitors.

– GPs retain responsibility for ensuring that access to confidential data in the practice is subject to appropriate controls so that it can be accessed only by practice staff who are providing care for patients and who have contracts of employment with the practice.[4]

1 The term 'processing' is extremely broad and encompasses holding, collecting, recording, obtaining or disclosing data or carrying out any operations on the data. In short, it is difficult to think of any activity in relation to data handling which would not be deemed as 'processing' under the DPA.
2 A data processor carries out data processing functions on behalf of the data controller.
3 Each GP practice will be a data controller for the information it holds.
4 An honorary contract does not provide a lawful basis for accessing confidential medical records for purposes other than direct patient care. In some limited circumstances, it might be appropriate for an individual to hold an honorary contract if they are assisting the practice with some aspect of direct care to patients and therefore have a legitimate relationship with patients, for example medicines management case identification.

Data controller responsibilities for 'fair and lawful processing'

– The first principle of the DPA requires data controllers to process the data they hold 'fairly' and 'lawfully'.

– Fairness requires data controllers to be open and transparent about how information will be used and that data are handled in line with what individuals would reasonably expect. GP practices therefore must provide information to their patients which must explain how their data are used, when they might be shared and with whom and who they should speak to about rights of objection.

– This does not generally require every patient to be informed directly but the Information Commissioner's Office (ICO) expects reasonable attempts to be made to inform patients about how their medical records are handled.

– The ICO suggests that a layered approach can be used. This means the provision of basic information available in different settings and formats with signposts to more detailed information, for example the practice website or leaflet.

– Every GP practice should have at least one notice prominently displayed on the practice notice board and on the practice website explaining that the practice holds medical records confidentially and primarily for the provision of direct patient care. The notice should explain when medical records might be used for purposes other than direct patient care. An example from the ICO is provided at Appendix 1. The practice could add to it as appropriate, for example, the notice might state that:

  'This practice contributes to medical research and may send relevant information to medical research databases such as the Clinical Practice Research Datalink and QResearch' when the law allows; and/or

  'This practice contributes to national clinical audits and may sometimes send relevant data to the Health and Social Care Information Centre (HSCIC) when the law allows'; and/or

  'In order to comply with its legal obligations this practice may send data to the Health and Social Care Information Centre when directed by the Secretary of State for Health'.

– It is important that the notice, often referred to as a 'privacy notice' or 'fair processing notice', is kept up to date and is clearly visible in the practice – not hidden under later notices. Some practices have electronic notice boards which are an excellent way to ensure that patients are informed about these important matters. In addition to the notice board some practices include information with repeat prescriptions.

– Failure to provide reasonable 'fair processing' information to patients could lead to a financial penalty from the ICO if a patient complained that they were unaware of how their data had been handled was upheld.

– The ICO website provides very useful information about fair processing and how transparency and openness can be demonstrated:[5] www.ico.org.uk

– For GP data controllers, the key component of 'lawful' processing is compliance with common law obligations of confidentiality.[6] When considering requests for access to confidential information without patient consent GPs must be confident that there is a lawful basis for the disclosure.

5 The ICO privacy notice code of practice is available on the ICO website.
6 The BMA has produced a toolkit on confidentiality which covers the main aspects of doctors' duty of confidentiality:

Flows of data from the practice

- In order to ensure that they can uphold their data controller responsibilities, it is important that GPs are clear about what data leave the practice via their IT systems.

- This might involve the practice carrying out an 'audit' of the data flows in which the practice participates in order to establish, for example:
  - the data flows which are in anonymous form;
  - the data flows which are in identifiable form (and the legal basis for these flows);
  - the data sharing agreements the practice has signed up to.

- When data flows have been clarified this should form part of the more detailed information on the practice website or leaflet to which patients are directed by the privacy notice. The information should include details on the nature of the data, who they are shared with and for what purpose and the legal basis for the sharing.

Dealing with requests for identifiable confidential information

- When considering sharing confidential information or when handling requests from organisations, it is important that GPs are confident that there is a clear legal basis for the disclosure. When an organisation is providing direct care[7] and has a legitimate relationship with an individual, the legal basis for sharing relevant information will be implied consent.[8]

- Implied consent cannot be relied upon for sharing confidential data with an organisation which is not providing direct care and does not have a legitimate relationship with a patient or a group of patients.

- Where there are proposals for use of identifiable confidential patient records for purposes other than direct care,[9] for example, risk stratification or provision of services to patient population as a whole, implied consent cannot be relied upon and another legal basis will be necessary. The requesting organisation should make it clear to the GP practice which legal basis is being relied upon.[10]

- Even where a legal basis for the disclosure is in place, where a substantial extraction of identifiable confidential patient records is proposed, practices will still need to comply with the fair processing obligations. In some cases, it might be advisable to inform patients directly via a letter, text or email where appropriate. Such decisions will need to be made on a case by case basis and it might be necessary for the practice to seek further advice from a Caldicott Guardian,[11] the ICO or an information governance specialist.

7 In line with GMC guidance, the term 'direct care' also covers local clinical audit undertaken by the team which has provided care and which has a legitimate relationship with the patient.
8 For example when a patient agrees to a referral from the GP practice to a hospital.
9 Often referred to as secondary uses of information or indirect patient care.
10 Explicit patient consent, approval under s251 of the NHS Act 2006 or certain statutory requirements under the Health and Social Care Act 2012 can provide a legal basis. The BMA has produced guidance on disclosures for secondary uses: http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records
11 A senior person responsible for protecting the confidentiality of patient information and providing advice to staff to enable appropriate information sharing.

Appendix 1

The ICO has provided the following wording which might form the basis of a privacy notice. A GP practice could add to it as appropriate.

How we use your information

Medical confidentiality is the cornerstone of trust between doctor and patient and we keep your records secure and confidential.

For your direct care either from the practice or within the NHS hospital service we imply your consent to pass on relevant clinical information to other professional staff involved in your direct care.

Only when there is a legal basis for the transfer of data we may pass limited and relevant information to other NHS organisations to improve the efficient management of the NHS or to aid medical research.

If you wish to see more information about this subject please visit our website at: xxxxxxxxx

If you wish to object to the use of your data for these 'secondary; uses please speak to: xxxxxxx

British Medical Association
BMA House, Tavistock Square, London WC1H 9JP
bma.org.uk

BMA 20150856