Notes for GPs

What are the responsibilities for data controllers?

The Data Controller:
A person who (alone, jointly or in common with other persons) determines the purposes for which and the manner in which, any personal data is to be processed.

This includes activities such as interpretation, the exercise of professional judgment, or significant decisions in relation to the uses to which the data can be put.

GPs are data controllers for their patients' data and even if they use a third party (working under a contract) to process the data for a specific purpose, for example risk stratification, they remain the data controllers and responsible for the safe handling of the data.

Where organisations are working together, such as a GP practice and a data processing organisation, it is essential there is documented contractual clarity about who is the data controller and who is the data processor. This condition may become especially relevant if, for example, there is a data breach or legal problem and in cases where there is a subject access request or a third party request for access, e.g., the police. All requests for access remain the responsibility of the data controller. Under the contract, the data processor will carry out the specific instructions from the data controller and the data processor will have no responsibility for the decision making relating to these data.

Caldicott Guardians:
Every NHS organisation which holds patient records is required by law to have a Caldicott Guardian. This is a named individual who is responsible for the decision making about the processing, dissemination and release of confidential medical data on behalf of the organisation. Every GP practice should have such a person and the registration form to register is available from cgcertgp.doc

More information about Caldicott Guardians is available at
www.connectingforhealth.nhs.uk/infogov/**caldicott**

Transfer of confidential patient data:
As data controllers, GPs have a responsibility under the Data Protection Act as well as the common law duty of confidence to protect confidential patient information from unlawful use.

In the context of direct care of a patient, there is a professional and recently a statutory duty to share relevant confidential medical information (patient confidential data or PCD) with other healthcare staff providing direct care to the patient. For direct care, patient consent can usually be implied. A patient agreeing to a referral to hospital will expect relevant information to be passed to the hospital consultant and their consent is implied. This consent is the legal basis for the transfer.

When passing PCD to other organisations for purposes other than direct care, implied consent cannot be relied upon and an alternative legal basis will be necessary. Medical research and risk stratification are two simple examples where PCD may be required but there must be a clear legal basis before the transfer can occur legally. Explicit consent from the patient, section 251 support to override the common law duty of confidence, or certain disclosures under the Health and Social Care Act 2012 can provide such a basis.

Before the transfer of PCD for reasons other than direct care, GP data controllers must be clear of the legal basis supporting the transfer.

GP data controller responsibility to inform patients about the use of their medical records – Fair Processing:
Under the first principle of the Data Protection Act, information held by a practice on behalf of patients must be used in a fair and transparent manner. This principle is often referred to as “fair processing”. In practice, processing means the collection, use, disclosure, retention and possibly deletion of patient information.

Practices have a responsibility to ensure that patients are aware of how their data is stored, used, the conditions under which it may be transferred, their rights of access to view their data (subject access) and their rights to object to the use of the data in certain circumstances (NHS Constitution).

The law is generally non specific as to exactly how this fair processing may be achieved, but the Information Commissioner’s Office (ICO) suggests that a layered approach should be used with basic and simple information available in several different settings and formats, but with signposts to more detailed information via the internet and websites.

Every practice must have at least one notice prominently displayed on the surgery notice board explaining that the practice holds medical records confidentially and securely and primarily they are used for the safe and effective delivery of direct care but that sometimes parts of the record may be used for the efficient management of the NHS or medical audit or medical research. This notice can then direct patients to the practice leaflet or the practice website where a more detailed description of the use of records can

be accessed. The notice board should also inform patients how and where they can register their dissent to share their record for indirect care.
Some practices have electronic noticeboards which are an excellent way to ensure that patients are informed of these very important matters. When there are proposals for a specific and substantial use of patient records for non direct care such as the integrated care projects, it is certainly advisable, although not mandatory for practices to consider informing patients by mass text, email or letter where that is possible. Advice should be sought from the organisation requesting the data as to the level of information to patients that will already be provided by them. Other factors to consider are the clarity and accessibility of information that has already been provided to patients by the practice already. Professional organisations (BMA ,, RCGP, GMC) or the ICO, are able to offer advice on these matters when there is doubt.

The Data Protection Act and the first fair processing principle do not require every patient to be informed directly, but the Information Commissioner's Office (ICO) will be looking to confirm that "reasonable" attempts have been made to inform patients about their records and their rights. Usually this will require more than a small notice on a board, often hidden under later notices.

Information must be kept up to date. Failure to make these reasonable attempts to inform patients could lead to a financial sanction on the practice from the ICO if a patient complained about how their data had been handled.

The ICO website (ico.org.uk) has very useful information about fair processing and how to show transparency.

The following wording is a suggested template from the ICO website:

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 ico.org.uk.

If you wish to object to the use of your data for these "secondary" uses please speak to: XXXXXXXXXX.

What is section 251 of the NHS Act 2006?

In 2002, the Control of Patient Information Regulations gave statutory power for an independent body (now the Confidentiality Advisory Group subcommittee of the Health Research Authority hra.nhs.uk) to set aside the common law duty of confidentiality under certain specific conditions, to allow the use of large quantities of confidential medical data to be used for certain specific purposes without the express consent of an individual.

In practice, this protects the data controller from breaching the common law by passing on PCD under the conditions specified and for the purpose specified. The legislation is permissive and not directive, so practices can choose whether or not to supply the data.

These Regulations are used in large research projects, large management audits (National audits) and large risk stratification projects.

If a GP practice receives a request for data citing “s251 approval” the requestor must provide the practice with the evidence that the approval is in place and the conditions attached to the approval.

Summary:
The dramatic increase in computing power has enabled the analysis of huge electronic datasets for the public good, the improved efficiency of the NHS and research into many medical conditions.

There is a public interest in such work, but the value of this work has to be balanced against the potential damage to the public trust in the principle of medical confidentiality .

The law relating to information governance is very complex, but it is very important that the simple rules highlighted in this paper are recognised and applied to maintain this public trust and keep practices safe from litigation.

If you require more information visit the websites below or refer to your professional organisation.

Useful websites

ico.org.uk
england.nhs.uk
nhs.uk/caredata
HSCIC.gov.uk
bma.org.uk
hra.nhs.uk
rcgp.org.uk
gmc-uk.org