CONFIDENTIALITY

AUDIT

Audit of confidentiality within the pharmacy

Patient confidentiality is at an increasing risk with larger patient care teams and everyone is affected. The introduction of national electronic health records will require careful safeguards to provide information to those who need it whilst also preventing unauthorised access. The extension of the role of pharmacists and others will sometimes require access to patient care records. The increased use of multidisciplinary teams to provide health care heightens the need for the sharing of information. Sometimes, clinical audit such as in relation to patient pathways, necessarily involves staff looking at patient identifiable information. New and proposed legislation provides for access to confidential information under certain conditions – so staff undertaking clinical audit are bound by the code of confidentiality.

Administrative procedures often threaten confidentiality. Patients expect that the information they supply about themselves, and that which is uncovered during the course of medical treatment, is kept confidential.

The Caldicott committee report describes principles of good practice to safeguard confidentiality when information is being used for non-clinical purposes:

- justify the purpose
- do not use patient identifiable information unless it is absolutely necessary
- use the minimum necessary patient identifiable information
- everyone with access to patient identifiable information should be aware of his or her responsibilities.

These principles are useful to keep in mind when dealing with clinical situations as well. Concerns about confidentiality prevent young people from attending general practices for help and advice about sexual matters and other health worries. You should know about the most recent advice about confidentiality and young people.

The Freedom of Information Act and Data Protection Act (see appendix 1) outline situations where confidential information can be shared and the procedures that are required to be in place to allow this to happen.

Anecdotal evidence suggests that some cultural or minority groups avoid attending general practice with their health problems (e.g. patients who are HIV positive) because of fears about confidentiality. These fears may seriously affect how well their health concerns are managed.

CRITERIA	Standard = poor	Standard = average	Standard = excellent
Information available on how information will be used	No information or simple posters and leaflets in waiting room	An active campaign in place to promote understanding of NHS information use	Active campaign includes arrangements for patients with special or different needs
Staff code of conduct for confidentiality	No code exists or staff are not generally aware of it	Code of conduct exists and all staff are aware of it	Code regularly reviewed and updated as necessary
Staff induction procedures for full and part-time staff, temporary staff, contracted staff	No mention of confidentiality and security requirements in induction for most staff	Basic requirements outlined as part of induction process for all staff	Understanding of the requirements of confidentiality and security is enhanced by training and comprehension is checked
Confidentiality and security training needs assessment	Training needs not assessed systematically for most staff	Training needs considered as a consequence of systems or organisational changes	Systematic assessment of staff training needs and evaluation of training already undertaken
Staff contracts	No confidentiality requirements included	Confidentiality requirements included for some staff	Confidentiality requirements included for all staff
Computer passwords	Not in place	In place but shared between members of staff. Not changed regularly	Only used by the individual, kept secret from others, not easily predicted, changed regularly
Discussing patient information	Discussed openly within pharmacy	Discussed in private areas only but can be overheard	Avoidance of discussion of patient information where it can be overheard
Patient identifiable information	No procedures in place	Procedures in place for when and how patient identifiable information is used	Individuals asking for patient information are being positively identified as being entitled to that information Patient identifying information is removed from documents unless there is a specific need for it.
Information flow is reviewed and monitored*	No procedures in place	Procedures in place for some information flows	Procedures in place for all patient identifiable information

STANDARDS

Standards should be:			
realistic	measurable	achievable	agreed

Possible standards are given in the chart overleaf. You should be aiming at the 'excellent' level, but be realistic about what you can achieve when you first start.

METHODOLOGY:

A. Design the audit

1. Selection of sample
You might carry out the observations as an individual within your practice, team or PCT, or collect data about confidentiality for which you have some managerial responsibility.

2. Prospective or retrospective
The audit has to be retrospective but contemporaneous because of the nature of the data.

3. Collecting the data
Record data on each of the criteria.

4. Who will collect the data?
Every member of your practice, team or PCT could collect data from their own experience and observation but it is possibly more manageable if the one person collects the data by looking at systems and discussing confidentiality with all team members.

5. Who will analyse and present the data?
The manager might take the responsibility.

6. Feedback and negotiate change
You should look at the changes required with all the practice team members involved. For example, the audit may indicate:

- No systematic training on confidentiality exists for current or new staff.
- Lack of protocols and training leads to variable application of controls over information dissemination
- Lack of imagination has resulted in lax security of medical information. Identifiable patient information can be seen by visitors and the public, computers are left unattended with passwords still logged in, and / or the identity of people asking for information by telephone is not clearly established.

7. Influencing changes resulting from the audit
The manager is responsible for monitoring whether the changes agreed are followed through and all individuals are responsible for their own change in behaviour or practice.

8. Planning to re-audit
If you find your standards are poor, then you need to make rapid changes and re-audit after a short interval e.g. 3 months. If your standards are excellent, the interval before you re-audit can be longer e.g. 12 months.

B. Resources required to complete the audit

- Extra time for making observations and recording the data.
- Designated time for the team to meet and discuss how the findings can be improved, moving towards the 'excellent' standard.

With acknowledgement to:
- Dr Ruth Chambers – Clinical Dean at Staffordshire University, professor of Primary Care Development Stoke-on-Trent teaching PCT and GP Adviser on GP recruitment and retention to Shropshire and Staffordshire Strategic Health Authority
- Dr Gill Wakley, freelance GP

Data Protection Act Summary

The Data Protection Act 1998, which came into force on 1st March 2000, regulates the processing of personal data. The Data Protection Act 1998 only covers the records of living patients and covers all of the UK. Both computerised and manual records are regulated by the Act.

There are eight data principles that the data controller has to comply with as set out in the Data Protection Act 1998. The principles require that the data be:

- Processed fairly and lawfully
- Obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Adequate, relevant and not excessive in relation to that purpose or purposes for which they are processed
- Accurate and, where necessary, kept up to date
- Not kept for longer than is necessary
- Processed in accordance with the rights of data subjects under this Act
- Protected against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Additional reading:

- Fact sheet twelve: Confidentiality, the Data Protection Act 1998 and the Disclosure of Information. http://www.rpsgb.org.uk/pdfs/factsheet12.pdf
- NHS code of practice on confidentiality and its relation to community pharmacy (England and Wales) http://www.pjonline.com/pdf/society/pj_20051029_nhscode.pdf