Issue: March 2016

PROFESSIONAL STANDARDS AND GUIDANCE FOR PATIENT CONFIDENTIALITY

Pharmaceutical Society of Northern Ireland

PROFESSIONAL STANDARDS AND GUIDANCE FOR PATIENT CONFIDENTIALITY

CONTENTS

Status of this document
About this document
1 Protection of Service User Information
1.1 Ethical obligations to protect patient privacy
1.2 Disability Discrimination Act 1995

2 Duty of confidentiality

3 Keeping information confidential
3.1 Data Protection Act (1998)
3.2 Preventing information being released accidentally
3.3 Disposal of patient identifiable information
3.4 Computer records
3.5 Notification to the Information Commissioner's Office
3.6 Pharmacy staff
3.7 Standard Operating Procedures

4 Disclosure of Information
4.1 Obtaining patient consent
4.2 Releasing the minimum amount of information necessary
4.3 Deceased patients

5 Releasing information without consent
5.1 Deciding to release information without consent
5.2 Exceptional circumstances (including those permitted by law)
5.3 Maintaining records

6 Northern Ireland Code of Practice on Confidentiality and Disclosure of Information

Guidance that support this document
Further reading
Acknowledgements

STATUS OF THIS DOCUMENT

This guidance is addressed to pharmacists but may also help patients and the public understand the nature and level of confidentiality that may be expected of their pharmacist.

Standard 2.1.12 of the Code states that a pharmacist must adhere to all relevant legislation, standards and guidance.

This document contains:

- mandatory professional standards (indicated by the word 'must' and 'have to') for all registered pharmacists;
  and
- guidance on good practice (indicated by the word 'should', 'might', 'may', 'would', 'will' and 'could') which should be followed in all normal circumstances.

Serious or persistent failure to follow this guidance will put a pharmacist's registration at risk. The pharmacist must, therefore, be prepared to explain and justify his[1] actions.

If a complaint is made against a pharmacist, the Pharmaceutical Society NI's, Fitness to Practise committee will take account of the requirements of the Code and underpinning documents, including this one. The pharmacist will be expected to justify any decision to act outside the terms set down in these documents.

ABOUT THIS DOCUMENT

The Code sets out the five mandatory principles of professional and ethical practice that a pharmacist must follow. It provides a framework for professional decision-making and it is the pharmacist's responsibility to apply the principles to daily work situations, using his professional judgement. The guidance is not meant to be exhaustive, nor can it be.

1 'Pharmacist' appears with masculine pronoun and is understood to refer to male/female gender.

Standard 1.3 of the Code states that a pharmacist must '***maintain and protect confidential information***'. In adhering to this standard, a pharmacist is expected to:

- respect the confidentiality of information, professional or otherwise, acquired in the course of professional practice or only use it for the purposes for which it is given and in compliance with current legislation.
- maintain systems which ensure security of information and take reasonable steps to prevent unauthorised access to it.
- ensure that all who have access to patient or service user's information know and maintain its confidential nature.
- ensure that confidential information is not disclosed without consent, except where legally required or permitted.

This document expands on the principles of the Code to explain the pharmacist's professional responsibilities when protecting patient privacy and the confidentiality of patient information.

A pharmacist has both a professional and legal duty to protect the privacy and confidentiality of patient information. This forms part of the general obligation to provide a service which is respectful of and actively promotes the human rights and dignity of patients.

This document does not give detailed guidance on legal requirements. The pharmacist must adhere to relevant legislative requirements set out in the Data Protection Act 1998, Human Rights Act 1998, the common law of confidentiality[2] and with any Health Service or employment policies that may apply to his work.

This guidance takes account of, and is consistent with current law in Northern Ireland.

All pharmacists should endeavour to keep themselves informed of any developments which may be relevant to their practice. Occasionally it may be necessary to ask for a professional legal opinion.

1 PROTECTION OF SERVICE USER INFORMATION

The general duty to maintain confidentiality and respect privacy is recognised by professional ethical codes which apply to health and social care staff including pharmacists and their staff and they abide by the Data Protection Act

1998. (See section 3.4).

2 The common law is the law that develops over time through the decisions of judges in particular cases. It is not included in an Act of Parliament.

1.1 ETHICAL OBLIGATIONS TO PROTECT PATIENT PRIVACY

The Department of Health, Social Services & Public Safety, Code of Practice on Protecting the Confidentiality of Service User Information clearly states that, *"The nature of the **obligation to protect confidentiality** can be expressed in terms of three core **ethical principles which underpin the law**:*

- *individuals have a **fundamental right to the privacy and confidentiality** of information related to their health and social care;*
- *individuals have a right to **control access to and disclosure of their own health and social care information** by giving, withholding or withdrawing consent;*
- *for **any disclosure** of confidential information health and social care staff should have a regard to its **necessity, proportionality and any risks attached to it[3]".***

An earlier draft of this document cited that, *"The **relationship between pharmacy staff and the service user** should be one of '**trust**'. Therefore within the relationship between a pharmacist or pharmacy staff and the patient, there exists a **tacit understanding** on the part of the patient that **private information will not be** further used or **disclosed without** the **awareness and consent** of the **patient.***

"Just as the patient has a right to self-determination in various other health and social care matters, it is in general the service-user's decision as to who should have access to personal health and social care information and how it may be used.

*"One reason for respecting confidences in health and social care is that doing so enables patients to disclose the sensitive information that staff need to provide treatment or care. **Without an assurance that confidentiality will be maintained, service-users might be less willing to disclose information,** resulting in obstacles to their effective care and negative effects for their health, for public health and for health and social care practice.*

*"**None of the arguments** stated above **lead to the conclusion that the ethical duty of confidentiality is absolute**. The confidentiality requirement exists within a wider social context in which members of staff have other duties, which may conflict with their duty of confidentiality. **In particular, they may have other ethical duties to disclose confidential information, without consent, if serious dangers are present for third parties or for the patient and where they judge that the disclosure of that information is likely to reduce or eliminate danger.** In assessing such risks and whether they outweigh the duty of confidentiality both the probability of the harm and its*

magnitude need to be considered. ***The ethical duty to disclose to prevent harm is greater when the combined weight of both the probability and the seriousness of harm to a third party or the patient are high***[4]*."*

1.2 DISABILITY DISCRIMINATION ACT 1995

Service providers are required under the Disability Discrimination Act 1995 to make reasonable adjustments to their policies, procedures and practices so that people with disabilities are not offered a service on less favourable terms than other members of society.

Human Rights legislation entitling people to privacy should also be borne in mind.

2 DUTY OF CONFIDENTIALITY STANDARDS

A patient has the right to expect that information obtained about him/her is kept confidential and is used only for the purposes for which it was given. This duty of confidentiality applies to all information obtained about a patient during the course of professional practice and extends to all members of the pharmacy team. Maintaining a patient's confidentiality is fundamental to the partnership between the pharmacist and the patient. A patient may be reluctant to seek advice from a pharmacist if he/she has concerns about the handling of confidential information.

Confidential information includes:

- personal details (including information that is not directly relevant to a patient's medical history);
- information about a patient's medication (both prescribed and non prescribed); and
- other information about a patient's medical history, treatment or care.

GOOD PRACTICE

For people with disabilities, confidentiality may be compromised if a patient finds him/herself obliged to ask a third party to read or explain information about the medication or dosage because the patient is unable to read or understand the information given to him/her.

3 DHSSPS "Code of Practice on Protecting the Confidentiality of Service User Information 29 January 2009. www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf
4 HSC, "Draft Code of Practice on Protecting the Confidentiality of Service User Information" 11 May 2007, Version 7.1, Page 7-8. www.dhsspsni.gov.uk/confidentiality-consultation-cop.pdf

If a pharmacist or member of staff in a pharmacy, knows or has reason to believe that a patient will not be able to read the information on packaging or patient information leaflets, he should take every step to eradicate the need for a patient to have to ask a third party to do this.

These steps will include:

- arranging for audio, large print or Braille versions of the Patient Information Leaflet to be made available to the patient as quickly as possible (e.g. through the X-PIL scheme);
- directing the patient to accessible websites or telephone information systems (e.g. the X-PIL scheme);
- writing dosage or other key information in a size and font which a patient can read;
- using compliance devices to help patients take the right medication at the right time;
- using differently sized or shaped containers for different medicines;
- taking additional time to explain the necessary information so that the patient can take it down in whatever way best suits them.

This list is not exhaustive, and the patient should always be asked which form of assistance, if any, he/she would like to receive. Please refer to www.rnib.org.uk.

3 KEEPING INFORMATION CONFIDENTIAL

3.1 DATA PROTECTION ACT (1998)

The Data Protection Act gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act works in two ways. Firstly, it states that anyone who processes personal information must comply with eight principles, which makes 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 an individual's rights;
- secure;
- not transferred to other countries without adequate protection.

The second area covered by the Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Should individuals or organisations feel they are being denied access to personal information they are entitled to, or feel their information has not been handled according to the eight principles, they can contact the Information Commissioner's Office[4 5] for help. Complaints are usually dealt with informally, but if this is not possible, enforcement action can be taken.

GOOD PRACTICE

For a patient experiencing any disability including, visual impairment, he/she will be denied his/her rights under the Data Protection Act if the eight principles contained within Act, or the means by which to raise a complaint, are not communicated to the patient in an accessible format appropriate for that patient.

Under the Data Protection Act an individual has the right to find out what personal information is held about him/her on computer or paper. For an individual with a visual impairment, information held about them on computer or on paper would need to be shown to them in an accessible format according to his/her personal choice in the event of that person making such a request.

3.2 PREVENTING INFORMATION BEING RELEASED ACCIDENTALLY STANDARDS

Accidental disclosure of information constitutes a breach of confidentiality. A pharmacist must take all reasonable steps to prevent accidental disclosure of, or unauthorised access to, confidential information. Robust procedures must be in place to protect the confidentiality of information the pharmacist receives, stores, sends or destroys. Patient identifiable information includes:

- the patient's name;
- postal address including postal code;
- date of birth;
- Health and Care number or local patient identifiable codes;

4 The Information Commissioner oversees adherence to the Data Protection Act 1998 and is also responsible for enforcing the Freedom of Information Act.

5 The Information Commissioner's Office – Northern Ireland, 51 Adelaide Street Belfast BT2 8FE Telephone: 028 9026 9380, Fax: 028 9026 9388, Email: ni@ico.gsi.gov.uk

- video footage; and
- anything else that can identify a patient either directly or indirectly such as rare diseases, drug treatments etc.

All records, registers, prescriptions and other sources of confidential information must be stored securely and be kept out of sight of patients, members of the public and any other person who should not have access to them. Security measures must be appropriate to the location where the confidential information is being stored.

The pharmacist must also take all reasonable steps to ensure appropriate levels of privacy for patient consultations so that confidential information is not overheard or accessed by others.

3.3 DISPOSAL OF PATIENT IDENTIFIABLE INFORMATION STANDARDS

Good records management and good professional practices are the essential basis of respect for the privacy of patient's information. In order to safeguard a patient's confidentiality, sources of patient-identifiable information must be disposed of in a way that prevents the information being accessible to unauthorised persons. This disposing should be done at a time consistent with an organisation's disposal schedule.

GOOD PRACTICE GUIDANCE

Disposing of patient identifiable information may involve cross-shredding, incineration, placing it in confidential waste or deleting the information with an indelible marker.

3.4 COMPUTER RECORDS STANDARDS

A patient has the right to expect that any computer record about him/her is held securely and is appropriately protected. The pharmacist is a data controller as per the Data Protection Act (1998) and must be satisfied that any system used is capable of restricting access. Suitable passwords, Personal Identification Number (PIN) or other restricted access systems must be in place. Any information stored about a person must be pertinent, accurate and up-to-date. Computers must be situated so that data cannot be seen intentionally, or by accident, by those who are not authorised to have access to it. Care must be taken in disposing of old computers to ensure that any confidential information/data is securely destroyed as far as possible.

GOOD PRACTICE GUIDANCE

- PIN numbers or passwords should not be shared and should be changed at regular intervals and on specific occasions (for example, if a member of staff terminates employment at the pharmacy).
- The level of access that various members of the pharmacy team have to a patient's records should be appropriate to their duties. For example, a member of staff who is responsible for ordering stock for the shop front will not need access to Patient Medication Records (PMRs) in the dispensary.

3.5 NOTIFICATION TO THE INFORMATION COMMISSIONER'S OFFICE (ICO)

STANDARDS

The processing of personal data, including the pharmacy PMR system, must be notified to the Information Commissioner's Office and records must be kept in accordance with relevant legislation. The ICO website provides guidance on the obligations of a data controller and specific guidance regarding the processing of health data.
(http://www.ico.gov.uk/upload/documents/library/data_protection/practical_app lication/health_data_-_use_and_disclosure001.pdf)

Unnecessary access to patient specific data must be prevented whether data is held electronically or in hard copy format. (Refer to Data Protection Act, 1998).

3.6 PHARMACY STAFF

STANDARDS

The pharmacist must ensure that all members of the pharmacy team are aware of, and demonstrate an understanding of, their duty to respect an individual's right to confidentiality and their obligations under the Data Protection Act (1998).

GOOD PRACTICE GUIDANCE

- Members of staff, where necessary, should understand that they have a duty to treat any information they receive in the course of their employment as confidential and failure to do so may result in disciplinary action. Employee contracts should include a confidentiality clause which should be signed by each member of staff. One copy should be retained on the personnel file and one copy retained by the member of staff.
- In the case of a pharmacist contacting another community pharmacy, general practice or nursing home requesting information about a

patient's medication history, only that information which is necessary to confirm patient identity and the nature of the request for a medication history should be provided. Other information such as the patient's current clinical condition should not be disclosed by the pharmacist.

3.7 STANDARD OPERATING PROCEDURES

STANDARDS

The way in which confidential information is handled must be taken into account when developing and reviewing standard operating procedures. Procedures must cover:

- who has access to confidential information and in what circumstances;
- how confidential information will be processed, used, stored and destroyed;
- disclosure of information; and
- maintenance of appropriate records of request for disclosure and details of the information disclosed.

4 DISCLOSURE OF INFORMATION

4.1 OBTAINING PATIENT CONSENT

STANDARDS

Information about a patient must not be disclosed without his/her consent other than in exceptional circumstances, or where required or permitted to by law, or by order of a Court. (See section 5 of this document). Where a patient allows the pharmacist to share information about him/her the pharmacist must make sure that the patient understands and does not object to:

- the information being released;
- the reason for the release;
- the categories of people and organisations to which the information will be released to; and
- how that information will be used.

GOOD PRACTICE

It is advisable that the pharmacist inform the patient of the nature and extent of the information to be shared and the need. In general, consent is required for the processing of sensitive personal data.

However, a patient will generally expect that information the pharmacist obtains in the course of his professional practice may be shared with other healthcare professionals or others who have a duty of confidentiality. The consent of the patient to the disclosure of information necessary for his/her care may be inferred from his/her acceptance of that care.

There may be occasions when a patient refuses to consent to particular information being shared with others providing care for him/her, for example, their general practitioner. Other than in exceptional circumstances the pharmacist must respect the patient's decision (see section 5.2 of this document). The patient must be made aware of the possible implications of not consenting to disclosure and his/her refusal to give consent must be documented.

Further information on obtaining consent can be found in the organisation's document, '*Standards and Guidance for Patient Consent*'.

4.2 RELEASING THE MINIMUM AMOUNT OF INFORMATION NECESSARY STANDARDS

When disclosing patient information, the pharmacist must release only the minimum amount of information necessary for the purpose. The pharmacist must use his professional judgement to consider the information needed to be disclosed, taking into account who is requesting the information and why.

If it is not necessary for the patient to be identified, the pharmacist must make sure that the information released by him does not inadvertently facilitate identification.

GOOD PRACTICE GUIDANCE

- Where appropriate, consideration should be given to the use of anonymised or encrypted data. [Note: anonymised/encrypted information is not considered to be confidential and its storage is not restricted in the same way as confidential information].
- In the case of a pharmacist who phones a fellow professional requesting a patient's drug information, the community pharmacist who accepts the call, must be satisfied that the individual he is speaking to, is known to him before disclosing confidential patient information (see section 5.2.2 and 5.3).

4.3 DECEASED PATIENTS STANDARDS

The confidential nature of a patient's information and the ethical obligation on pharmacy staff to respect that confidentiality remain after the death of a patient. As in life, the duty to maintain confidentiality of patient information after death is not absolute, but is subject to ethical and legal limitations. Even though the patient can no longer be harmed directly there is still a public interest in the maintenance of his/her privacy after death. A deceased patient's surviving friends and relatives might be harmed by disclosures, too, and it is they who might take action for a breach of confidentiality. {See *Lewis –v- SOS for Health [2008] EWHC 2196 QB*[6]}.

A competent patient can give or withhold consent to disclosure of information before his/her death and such wishes should be respected as they would in other circumstances. In particular, where a patient has made an explicit request before his/her death that confidential information should not be disclosed, then the patient's request should normally be upheld.

The '*Access to Health Records (Northern Ireland) Order 1993*' governs access to the health records of deceased patients.

5 RELEASING INFORMATION WITHOUT CONSENT

5.1 DECIDING TO RELEASE INFORMATION WITHOUT CONSENT STANDARDS

Confidential information must only be disclosed without consent **in exceptional circumstances or when permitted or required by law**, for example, where disclosure is by an order of the court, or where the public interest overrides the need to keep information confidential. Examples of circumstances where information may be disclosed without consent are detailed in section 5.2 of this document. Before releasing information without consent the pharmacist must, where practical or appropriate, endeavour to persuade the patient either to release information him/herself, or give permission to release it.

6 **Lewis v Secretary of State for Health [2008] EWHC 2196 (QB) (QBD)**. Under its general powers the court authorised the disclosure of the medical records of certain deceased patients to the Redfern Inquiry into human tissue analysis in United Kingdom nuclear facilities. A duty of confidentiality was capable of surviving the death of the confider. In the circumstances of the instant case, the duty of confidence had not survived the death of the confider. As to the legal foundation for authorisation, the statutory basis for authority to disclose the material sought would be rejected. The instant case was an appropriate case in which to hold that the public interest in disclosure of the material sought outweighed the other public interest, namely, that of maintaining the confidentiality of medical records and information, provided proper safeguards were put in place to ensure that no inappropriate information became public. Accordingly, disclosure of the medical records would be granted under the court's general powers.

If the pharmacist decides to reveal confidential information without obtaining consent he must be prepared to justify his decision and any action taken as a consequence of that decision.

5.2 EXCEPTIONAL CIRCUMSTANCES (INCLUDING THOSE PERMITTED OR REQUIRED BY LAW)

Information can be disclosed without patient consent in the following circumstances, including:

5.2.1 Where the patient's parent, guardian or carer has consented to the disclosure and the patient is deemed by law to be, or appears to be, incapable of consenting.

The organisation's document *Standards and Guidance for Patient Consent* provides information on determining a patient's capacity to provide consent.

Consideration should be taken of assessments already made by colleagues, for example, the patient's GP or an independent legal advisor.

5.2.2 Where disclosure of the information is to a person or body with a statutory right to require disclosure.

STANDARDS

Where the pharmacist is required to disclose information he does not have to obtain consent prior to disclosure. He must ensure that he releases the information only to an authorised person who is requesting disclosure in the performance of their statutory duties.

GOOD PRACTICE GUIDANCE

- *All reasonable efforts should be made to tell the patient that information will be released, why it is being released and to whom it is being released.*

5.2.3 Where disclosure is directed by HM Coroner, a judge or other presiding officer of a court, Public Prosecution Service in Northern Ireland, Crown Prosecution Office in England and Wales or Procurator Fiscal in Scotland.

STANDARDS

A court may order the pharmacist to release patient information without consent. If so, he must release only the minimum information needed to follow the order. In certain situations, his refusal to disclose information could result in him being found in contempt of court.

GOOD PRACTICE GUIDANCE

- *The pharmacist should, where possible, seek further legal or specialist advice in these situations.*

5.2.4 To a police officer or Health Service fraud investigation officer who provides in writing confirmation that disclosure is necessary to assist in the prevention, detection or prosecution of serious crime.

STANDARDS

There may be occasions where obtaining patient consent prior to disclosure will be inappropriate, for example, the pharmacist may receive a request for information believed to be necessary in the prevention or investigation of serious crime, in a situation where attempting to obtain consent may allow time for destruction of evidence. The request to disclose such information must be made in writing, with a clear statement of the purpose for which the information is required.

GOOD PRACTICE GUIDANCE

- *When faced with requests from the Police or a Health Service fraud investigation officer the pharmacist should consider whether there are any alternative sources for the information being requested that would not cause a breach of trust between him and the patient. The pharmacist should also discuss the matter with the person making the request and be satisfied that without disclosure, the investigation would be delayed or prejudiced.*

5.2.5 Where necessary to prevent serious injury or damage to the health of a patient, a third party or to public health.

GOOD PRACTICE GUIDANCE

- *The pharmacist should discuss with the patient the implications of continuing to undertake the activity that may cause serious injury or damage.*

5.2.6 Where disclosure is necessary for the protection of an adult or child lacking capacity.

STANDARDS

Where abuse or neglect of a person is suspected, that person's well-being is of utmost importance and ensuring this must be the pharmacist's prime concern.

GOOD PRACTICE GUIDANCE

- *The pharmacist should attempt to encourage the person to consent to disclosure; should he/she refuse the pharmacist will need to use his professional judgement to determine the best course of action.*
- *The pharmacist should consider speaking with other healthcare professionals who are also involved in the patient's care, for example, his/her general practitioner.*

The pharmacist should consult the Information Commissioner's Office[7] where he has queries about the appropriateness of disclosure in any of the above circumstances.

7 The Information Commissioner's Office – Northern Ireland, 51 Adelaide Street Belfast BT2 8FE Telephone: 028 9026 9380, Fax: 028 9026 9388, Email: ni@ico.gsi.gov.uk

***CIRCUMSTANCES* WHERE DISCLOSURE CAN TAKE PLACE *WITHOUT* PATIENT CONSENT:**

- where the patient's parent, guardian or carer has consented to the disclosure and the patient is deemed by law to be, or appears to be, incapable of consenting;
- where disclosure of the information is to a person or body with a statutory right to require disclosure;
- where disclosure is directed by a coroner, judge or other presiding officer of the court, Public Prosecution Service in Northern Ireland, Crown Prosecution Office in England and Wales and Procurator Fiscal in Scotland;
- to a police officer or Health Service Fraud Investigation Officer who provides in writing confirmation that disclosure is necessary to assist in the prevention, detection or prosecution of serious crime;
- where necessary to prevent serious injury or damage to the health of the patient, a third party or to public health; and
- where disclosure is necessary for the protection of a child or adult lacking capacity.

5.3 MAINTAINING RECORDS STANDARD

When the pharmacist makes a decision to disclose information without consent, he must keep an accurate record of:

- the identity/role of the person making the request;
- the reasons for releasing the information without patient consent;
- the extent to which he attempted to obtain patient consent, if at all;
- reasons for not seeking consent;
- reasons given by the patient for refusing consent;
- what information was disclosed.

If a patient refuses to provide consent in one situation the pharmacist must not assume that he/she will refuse to provide consent for disclosure in the future, in either matching or differing circumstances.

6 NORTHERN IRELAND CODE OF PRACTICE ON CONFIDENTIALITY AND DISCLOSURE OF INFORMATION STANDARDS

In January 2009, the Department of Health, Social Services and Public Safety (DHSSPS) published a Code of Practice on Confidentiality and Disclosure of Information. The aim of this Code is to support all staff who provide health and social care services in making good decisions about the protection, use and disclosure of patient information.

The Code of Practice on Confidentiality and Disclosure of Information can be viewed at: http://www.dhsspsni.gov.uk/confidentiality-code-of¬practice0109.pdf.

This, and other relevant standards or guidance on patient confidentiality, must be adhered to unless the pharmacist has good reason not to do so.

GUIDANCE THAT SUPPORTS THIS DOCUMENT

The following documents or guidance bulletins should be considered in conjunction with these standards:

- The Code – professional standards of conduct, ethics and performance for pharmacists (2016);
- Professional Standards and Guidance for Patient Consent;
- Protection of children and vulnerable adults (POCVA).

FURTHER READING

- "Guidance on NHS Code of Practice on Confidentiality" 29 October 2005, The Pharmaceutical Journal (Vol. 275) P 557 – 558.
- ACCESS to Health Records (Northern Ireland) ORDER 1993.
- The NPA Guide to Data Protection and Confidentiality in Community Pharmacy, September 2006.
- Wingfield Joy and Badcott David. Pharmacy Ethics and Decision Making. 2007. Grayslake, IL: Pharmaceutical Press 313. ISBN:9780853696896.
- Disability Discrimination Act 1995
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Caldicott Principles
- Code of Practice on Confidentiality and Disclosure of Information can be viewed at: http://www.dhsspsni.gov.uk/confidentiality-code-of-practice0109.pdf
- www.psnc.communitypharmacynews/freedomofinformationact2000. July 2007
- www.psnc.communitypharmacynews/dataprotectionact1998. August 2007

ACKNOWLEDGEMENTS

GMC
NPA
Information Commissioner's Office, Belfast
RNIB