INTRODUCTION

Health professionals have a duty of confidentiality regarding patient information.[1] However, the priority is to ensure that all relevant information necessary is clearly and accurately passed to others when this is necessary for the ongoing care of the patient.

The different aspects of legislation relating to these issues at times appear to conflict with each other. This guidance provides a brief overview of the relevant legislation under the following headings:

- patient identifiable information
- Data Protection Act
- NHS Policy
- protecting patient information
- patients' rights of access to personal health records
- disclosure to other bodies and organisations
- research
- consent
- further reading
- references.

PATIENT IDENTIFIABLE INFORMATION

This is any information that may be used to identify a patient directly or indirectly. It may include:

- patient's name, address, post code or date of birth
- any image or audio tape of the patient
- any other data that has the potential, however remote, that the patient may be identified from it (e.g. rare diseases, drug regimes, statistical analysis of small groups)
- patient record number
- combinations of any of the above increase the risk of a breach of confidentiality,[2] and include all verbal, written and electronic disclosure, whether formal or incidental.

DATA PROTECTION ACT

The main principles of the Data Protection Act 1998[3] should be read in conjunction with this guideline. The Act describes processes for obtaining, recording, holding, using and sharing information.

- Patients must be informed and give consent to any sharing of their personal information. Exceptions to this general rule may exist (**see sections on Disclosure, and Consent**).

Only the minimum amount of data should be collected and used to achieve the agreed purpose.

Information can only be retained for as long as it is needed to achieve its purpose.

Strict rules apply to the sharing of information.

NHS POLICY

All NHS employees must be aware of, and respect a patient's right to, confidentiality.[1,2] A disciplinary offence may have been committed for any behaviour contrary to their organisation's policy or the *NHS Code of Practice: Confidentiality* (in Scotland, the *NHS COP on Protecting Patient Confidentiality)*. Clinicians should be aware of how to access training, support or information they may need and be able to show that they are making every reasonable effort to comply with the relevant standards.[1,2]

PROTECTING PATIENT INFORMATION

There are five essential steps that Ambulance Clinicians and support staff, need to take to ensure that they comply with the relevant standards of confidentiality:

1. Record patient information concisely and accurately.

Inaccurate patient clinical records may contain false information about the patient concerned, for example by omission, error, unfounded comment or speculation. This breaches standards and brings the professional integrity of the ambulance clinician and the organisation into question.

2. Keep patient information physically secure.

The ambulance service has particular difficulties in ensuring that information is not shared accidentally with the public. Not only must any care the patient received be treated confidentially, the information gained must not be disclosed to anyone else unless to do so genuinely promotes patient care. Comments to the public must be guarded. Patient handover information should not be overheard or shared with those not directly involved in the patient's ongoing treatment. Patient records, either electronic or written, must be protected against unwarranted viewing, thus patient clinical records must be shielded from the view of others, stored securely after treatment, and only handed over to those with direct patient care or supervisory responsibility, or authorised ambulance service officers. Discussion about each case/patient must not disclose personal information unless there is genuine and provable health benefit.[2]

3. Follow guidance before disclosing any patient information

It is not sufficient for clinicians to understand the basic principles of confidentiality alone. They must also understand and comply with their organisation's requirements for information sharing. Similarly, it is the responsibility of each service to ensure that data-sharing policies are produced, communicated, monitored, updated and reviewed.[1] If there is any doubt about the sharing of information, there must be a Data Protection Officer and/or a Caldicott Guardian available to advise.[4,5]

4. Conform to best practice

All grades of Ambulance Clinicians come into contact with the public and other NHS disciplines. Any temptation to share information unnecessarily with other people who are known to them must be avoided, as the responsibility lies firmly with the holder of the data, both individually and organisationally.[6] A commitment to best practice should be applied to all patient information in any form, e.g. patient records, electronic data, surface mail, email, faxes, telephone calls, conversations that may be overheard, private comments to friends or colleagues.[7]

5. Anonymise information where possible

Patient information is said to be anonymised when items such as those in section 1 are removed.[1-3] It means that the patient cannot be identified by the receiver of the information and any theoretical possibility of recognition is extremely small. Anonymise patient confidential data wherever possible and reasonable. If information is recorded, retained or transmitted in any way, it should be anonymised unless to do so would prevent any genuine health-benefit reasons for its collection/storage.[1, 2]

PATIENTS' RIGHTS OF ACCESS TO PERSONAL HEALTH RECORDS

Patients have a right to see, and obtain a copy of personal health information held about them.[8] This includes any legally appointed representative and those with parental responsibility for young patients. Children also have this right provided they have the capacity to understand the information. Ambulance Services have a right to charge for this information; guidelines exist for this.[3]

There are exceptions to patients' rights to see their personal health information. If the data could identify someone else and such data cannot be removed from the record, it is subject to legal restrictions. If access to data could cause serious harm to the patient or someone else's physical or mental well-being then the request can be refused.[1,8,9] Within ambulance service operations, these instances are extremely rare. If there is doubt about whether such exceptions exist, the Caldicott Guardian or Data Protection Officer should be consulted and agreement reached with the patient's lead clinician.[9]

Notwithstanding the exceptions noted above, clinicians should make every effort to support a patient's right to gain access to their personal health data. It is a requirement that such data should be received by the patient within 40 days of the request. To enable this, services should have clear written procedures in place to deal with such requests.[3]

DISCLOSURE TO OTHER BODIES AND ORGANISATIONS:

Police

The police have the right of access to personal information (name, address etc) in the investigation, detection and prevention of **any** crime. They also have the right of access to confidential health information (type of illness or injury etc.,) in the investigation, detection or prevention of a **serious** crime (rape, terrorism, murder etc).

They have no right to expect to receive information where criminality, clinician safety and public safety are not involved. Generalised information regarding attendance at an incident **may** be passed to the police through locally agreed procedures, where details of the incident location and what is involved may be disclosed – but passage of personal or confidential health data **may not**.

Fire Service and Other Emergency Services

There is no right of access for emergency service personnel other than the police to a patient's personal health information.[2] Situations may occur where clinicians feel that such disclosure would be in the best interests of the patient, or that by not disclosing it, other emergency workers could be put at risk. Clinicians should follow the best practice advice given in the section above on NHS Policy on such occasions. Otherwise, data access should be governed by formal documented requests and consideration by the Data Protection Officer and/or the Caldicott Guardian.

The Media

There is no basis for disclosure of confidential or identifiable information to the media. Services may receive requests for information in special circumstances, e.g. requests for updates on celebrity patients or following large incidents, when answering press statements (Public Interest exemption). In such instances, the explicit consent of the 'data subjects' should be gained and recorded prior to any disclosure.[2]

For Commercial Purposes

Ambulance Services are not registered to use patient information for primarily commercial purposes. If such use was permitted, each patient would need to give explicit consent for their data to be used within the commercial setting and be given an "opt out" facility. This would need to include all intended purposes of all parties to the agreement and lists of all persons/groups who would have access to the data.[3] Due to the nature of commercial enterprise, this consent would need to be explicit (expressly and actively given) as opposed to implied (acceptance without voicing an objection).

RESEARCH

All data for research should be anonymised wherever possible. If anonymisation would be contrary to the aims of the research, prior consent must be gained. Formal research guidelines exist for the use of health data and these must be consulted.

CONSENT

Consent and patient confidentiality are inextricably linked. In essence, the patient is said to be the owner of his/her own personal, non-anonymised patient data and therefore needs to give approval before it is used by other people.[9] There are exceptions to this general rule:

- There may be legal requirements to disclose data without consent, e.g. due to **notifiable diseases**. Even then, however, the patient must be informed that this has been executed.[3]
- Where there is a risk to the patient's well being by not informing other professionals without consent, e.g. where a **child or vulnerable adult may be in need of protection** and informing the relevant authorities would appear to safeguard the patient's best interests.
- **Inability to consent**, e.g. some children, adults who lack capacity or patients who are seriously ill or injured and who could reasonably be expected to give consent if it were otherwise possible to do so. Even in such circumstances, data must be used cautiously and anonymised where possible. If a proxy, guardian or parent is available, they should be consulted.[2]
- Use of personal information without consent may be justified if it is in the **public interest** to do so. This may occur to prevent or detect a serious crime, for example.

In all the above instances, the advice of a Service Caldicott Guardian and/or Data Protection Officer should be sought prior to the use or release of any personal health data.

Key Points – Patient Confidentiality

- Health professionals have a duty of confidentiality regarding patient information. The priority, however, is to ensure that all relevant information is passed to others to ensure ongoing patient care.
- Patient information must be recorded accurately, kept physically secure, and anonymised whenever possible.
- Follow guidance before disclosing any patient information. Data Protection Officers and Caldicott Guardians are there to assist.
- Emergency situations may call for the sharing of patient information with other, mainly emergency-agencies. Follow best practice and act in the best interest of the patient.
- Ensure you are aware of your Service rules for patient confidentiality and follow them – but remember that ongoing patient care should never be compromised in their application.

REFERENCES

[1] Health Professions Council. Standards of conduct, performance and ethics: Your duties as a registrant London: Health Professions Council 2003.

[2] NHS Scotland Code of Practice on Protecting Patient Confidentiality. Edinburgh: Scottish Executive Health Department. Available from:http://www.confidentiality.scot.nhs.uk/, 2003.

[3] Data Protection Act 1998 1998.

[4] NHS Executive. Report on the Review of Patient-identifiable Information – December 1997 (Caldicott Report). London: : HMSO, 1999.

[5] Brooks J. Caldicott Guardians – driving the confidentiality agenda. *Br J Healthcare Comput Info Manage* 2004;21(3):20-1.

[6] Thomas G. Team learning: the issue of patient confidentiality *Work Based Learning in Primary Care* 2004;2(4):377-380.

[7] Medical Defence Union. Confidentiality: Medical Defence Union: London. Available from:ttp://www.the-mdu.com/gp/search/searchresults.asp, 2001.

[8] General Medical Council. Confidentiality: protecting and providing information: General Medical Council: London. Available from: http://www.gmc-uk.org/guidance/library/confidentiality.asp, 2000.

[9] Woogara J. Patients' rights to privacy and dignity in the NHS. *Nurs Stand* 2005;19(18):33-7.

Further Reading

The principles within the following documents have significant impact on patient confidentiality issues, and should be considered essential reading.

- Health Professions Council. Standards of conduct, performance and ethics: Your duties as a registrant: London: Health Professions Council 2003.
- NHS Scotland Code of Practice on Protecting Patient Confidentiality. Edinburgh: Scottish Executive Health Department. Available from:http://www.confidentiality.scot.nhs.uk/, 2003.Data Protection Act 1998
- Also, ***refer to consent guideline.***

METHODOLOGY

Refer to methodology section; see below for patient confidentiality search strategy.

Patient confidentiality strategy

Electronic databases searched:

CINAHL(Ovid) – years search 82 - 05

EMBASE (Ovid) – years search 80 - 05

MEDLINE (Ovid) – years search 66-95

MEDLINE (Ovid) – years search 66-05

ERIC (Ovid) – years search 66-05

EBM Review – years search All

AMED – years search 85 - 05

Search strategy:

MEDLINE	CINAHL	OTHERS
1. controlled.ab.	1. meta analysis/	1. meta.ab.
2. design.ab.	2. systematic review/	2. synthesis.ab.
3. evidence.ab.	3. systematic review.pt.	3. literature.ab.
4. extraction.ab.	4. (metaanaly$ or meta-analy$).tw.	4. randomized.hw.
5. randomized controlled trials/	5. metanal$	5. published.ab.
6. meta-analysis.pt.	6. information.pt.	6. meta-analysis.pt.
7. review.pt.	7. (review$ or overview$).ti.	7. extraction.ab.
8. sources.ab.	8. literature review/	8. trials.hw.
9. studies.ab	9. exp literature searching/	9. controlled.hw.
10. or/1-9	10. cochrane$.tw.	10. search.ab.
11. letter.pt.	11. synthes$.tw. adj3 (literature$ or research$ or studies or data).tw.	11. medline.ab.
12. comment.pt.	12. (medline or medlars or embase or scisearch or psycinfo or psychinfo or psyclit or psychlit).tw,sh.	12. selection.ab.
13. editorial.pt.	13. pooled analy$.tw.	13. sources.ab.
14. or/11-13	14. ((data adj2 pool$) and studies).tw.	14. trials.ab.
15. confidentiality.ab.	15. ((hand or manual$ or database$ or computer$) adj2 search$).tw.	15. review.ab.
16. 10 not 14	16. reference databases/	16. review.pt.
17. 15 and 16	17. ((electronic$ or bibliographic$) adj2 (database$ or data base$)).tw.	17. articles.ab.
	18. (review or systematic-review or practice-guidelines).pt.	18. reviewed.ab.
		19. english.ab.
		20. language.ab.
		21. comment.pt.
		22. letter.pt.
		23. editorial.pt.
		24. animal/
		25. human/
		26. 24 not (24 and 25)

MEDLINE	CINAHL	OTHERS
	19. (review$ or overview$).ab. 20. (systematic$ or methodologic$ or quantitativ$ or research$ or literature$ or studies or trial$ or effective$).ab. 21. 18 and 20 22. 19 adj10 20 23. or/1-17,21,22 24. editorial.pt. 25. letter.pt. 26. case study.pt. 27. record review/ 28. peer review/ 29. (retrospective$ adj2 review$).tw. 30. (case$ adj2 review$).tw. 31. (record$ adj2 review$).tw. 32. (patient$ adj2 review$).tw. 33. (patient$ adj2 chart$).tw. 34. (peer adj2 review$).tw. 35. (chart$ adj2 review$).tw. 36. (case$ adj2 report$).tw. 37. exp case control studies/ 38. exp prospective studies/ 39. case studies/ 40. human studies/ 41. "edit and review"/ 42. (adults$ or children).tw. 43. or/24-42 44. 43 not (43 and 23) 45. 23 not 44 46. patient AND confidentiality 47. 46 and 45	27. confidentiality 28. 27 not (21 or 22 or 23 or 26) 29. or/1-20 30. 28 and 29

Additional sources searched:

BNID - British Nursing Index – http://ds.datastarweb.com/ds/products/datastar/sheets/bnid.htm

British Medical Journal – http://bmj.bmjjournals.com

Centre for Reviews and Dissemination - http://www.york.ac.uk/inst/crd/crddatabases.htm

Department of Health – http://www.dh.gov.uk/Home/fs/en

Healthline – http://www.healthline.com

Health Politics – http://www.health-politics.com

LawDepot – http://legal.dotheresearch.com

Netreach – http://www.netreach.co.uk

Nurse-aide – http://www.nurse-aide.com

Official Documents Archive – http://www.archive.official-documents.co.uk

Office of Public Sector Information – http://www.opsi.gov.uk

The Cochrane Library – http://www.update-software.com/publications/cochrane

Reference sections from relevant articles were searched.