



Faculty of Sexual and Reproductive Healthcare
of the Royal College of Obstetricians and Gynaecologists

SERVICE STANDARDS ON CONFIDENTIALITY

Reviewed & updated: January 2009

Review Date: January 2012

27 Sussex Place, London, NW1 4RG
www.fsrh.org

Published by Clinical Standards Committee

Faculty of Sexual & Reproductive Healthcare
of the Royal College of Obstetricians and Gynaecologists

Committee Members:

Dr Asha Kasliwal, Chair

Dr Louise Massey, Vice Chair

Dr Ailsa Gebbie, Ex-Officio

Dr Jane Dickson

Dr Jagruti Doshi, Trainee member

Dr Val Godfree

Ms Lynn Heeney

Dr Wendy Higson

Dr Kate Nash

First Published March 2005

Updated January 2009

Review date: January 2012

**SERVICE STANDARDS
ON
CONFIDENTIALITY**

- 1. Standard Statement on Confidentiality Policies** **Page 6**

All services should have a written Confidentiality Policy.
- 2. Standard Statement on Confidentiality Training** **Page 8**

Services should provide all staff with a programme of Training on Confidentiality.
- 3. Standard Statement on Clients Rights to Confidentiality** **Page 9**

All clients have the right to expect that information about them will be held in confidence.
- 4. Standard Statement on Sharing Non-identifiable Information** **Page 10**

Services should ensure that clients are informed that anonymised information may be used for service improvement, audit and clinical Governance purposes.
- 5. Standard Statement on Working with Young People** **Page 11**

Services should ensure that their staffs are aware that all people, irrespective of age, are entitled to the same duty of confidentiality, provided they understand the implications of the advice and treatment offered.
- 6. Standard Statement on Disposal of Confidential Information** **Page 12**

All services should have mechanisms for disposal of confidential information.
- 7. Standard Statement on Disclosure without Consent** **Page 13**

Services should inform clients that Personal information should only be disclosed if it is in the public interest, or to protect the individual.

SERVICE STANDARDS ON CONFIDENTIALITY

Introduction

Patient information is generally held under legal and ethical obligations of confidentiality. Patients entrust the NHS or allow it to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service. This is of particular importance to matters relating to sexual and reproductive health

Sexual & Reproductive Healthcare Services have an excellent track record as far as confidentiality is concerned, but services need to keep up to date with current national policies and guidance. The core guidance document is the NHS Confidentiality Code of Practice¹ with which all staff should be familiar as it is a guide to required practice for all those working within or under contract to NHS organisations. This Code has been endorsed by the Information Commissioner, General Medical Council (GMC), British Medical Association (BMA) and the Medical Research Council. In addition, all staff should be aware of the NHS Code of Practice on Information Security Management 2007² and the document Joint Guidance on use of IT equipment and access to patient data published by the DH, GMC and Information Commissioner³. The duty of confidence must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures

All healthcare professionals must maintain the standards of confidentiality laid down by their professional body, such as the GMC or Nursing and Midwifery Council (NMC), or risk complaint for professional misconduct. Breach of confidence, inappropriate use of health records or abuse of computer systems may result in a warning, restriction of practice, removal from the register, and possibly result in legal proceedings.

The term “service” is used in this document to denote any provider of Sexual & Reproductive Healthcare services, i.e. it includes services in general practice, community clinics and hospital-based settings. The standards apply to all NHS organisations, including NHS Foundation Trusts, and private/independent and voluntary providers of NHS care. Throughout this document the term “staff” is used to mean all personnel, whether paid or voluntary, who are involved in the delivery of the service. This includes volunteers and visitors to services as well as students and trainees.

The Faculty has already published a document on Service Standards for Sexual Health Services⁴, which includes a standard on confidentiality. This paper seeks to expand on the initial statement, to cover guidance from the Department of Health (DH)^{1,2,3,5,6,7,8} General Medical Council (GMC)^{9, 10} other professional organisations^{11,12,33,41}. The Department of Health published “Standards for Better Health”⁵ in 2004 and this states as Core Standard C13: Health care organisations must have systems in place to ensure that:

- staff treat patients, their relatives and carers with dignity and respect;
- appropriate consent is obtained when required for all contacts with patients and for the use of any patient confidential information;
- staff treat patient information confidentially, except where authorised by legislation to the contrary.

Clients need to know that personal information is secure and that it is handled with care and respect by health professionals, but confidentiality does not mean that information cannot be shared. It is paramount that clients understand why and in what circumstances information needs to be passed on to others and whether it will be identifiable or anonymous.

Individuals already have the right to access their own personal information under the Data Protection Act, 1998¹³. The Freedom of Information Act¹⁴, 2000 extends this to allow access to all types of public

information. It is important that clients understand that the protection of their identifiable personal information always overrides this.

Fundamental to the whole of this document is the existence of a written confidentiality policy for every service. Guidance is given as to the content of the policy. In particular, sexual and reproductive healthcare service providers need to be aware of the possibilities of inadvertent breaches of confidentiality, e.g. overhearing of conversations between staff, overhearing of telephone conversations between staff and clients, information seen on computer screens, fax machines etc. It is essential that clerical and other non-clinical staffs are as conversant with confidentiality issues as clinical staff. A sample confidentiality policy, agreement and statement, together with staff training modules are available in the RCGP /Brook publication "Confidentiality and young people toolkit"³³

Confidentiality is a Clinical Governance issue – serious breach of confidentiality by NHS employees carries with it severe penalties. The Caldicott principles^{15, 16} should always be followed:

- justify the purpose
- don't use patient identifiable information unless it is absolutely necessary
- use the minimum necessary patient identifiable information
- access to patient identifiable information should be on a strict need to know basis
- everyone should be aware of their responsibilities
- understand and comply with the law

There are three areas of law that are most relevant to the processing of patient information. These are:

1. The Human Rights Act 1998¹⁷

- Article 8 of the Human Rights Act establishes a right to 'respect for private and family life'. Anyone who processes patient information must do so for necessary and legitimate purposes or be in breach of the Act.

2. The Data Protection Act 1998¹³

- The Data Protection Act regulates how data about identifiable individuals may be processed. It contains eight principles and a number of other relevant sections, the most significant of which in this context are:
 - 2.1 the 1st Principle which requires data processing to be fair to the individual concerned and lawful in terms of wider UK law.
 - 2.2 the 7th Principle which requires those responsible for personal data to protect it against unauthorised or unlawful processing and against accidental loss, destruction or damage. It also requires that security measures must be commensurate with the nature of the data and the harm that may be suffered from a breach of security. Steps must also be taken to ensure that staff with access to the data are reliable.
 - 2.3 section 55 which makes it a criminal offence to obtain or disclose personal data unlawfully.

3. The Common Law of Confidentiality

Although not codified in an Act of Parliament, common law is built up from case law where practice has been established by individual judgements. The key principle is that information confided for the purpose of receiving care and treatment should not be processed for other purposes except in circumstances where the law permits or requires it. The great majority of health professionals take their responsibility for safeguarding clinical patient information extremely seriously and appreciate the obligations of confidentiality that apply. However although non-clinical patient contact details are, in most cases, not held under legal obligations of confidentiality, this is not the case for all patients so it is Department of Health policy to treat demographic data held within the Personal Demographic Service as if it were.

The Information Commissioner is the independent authority responsible for overseeing and governing the Data Protection Act 1998 and the Freedom of Information Act 2000. He has a range of duties including promotion of good information handling and encouragement of codes of practice for data Service Standards on Confidentiality

controllers (those who decide how and why personal data are processed). His web site provides guidance on general issues relating to data protection and freedom of information, but also provides a large amount of health-specific guidance. <http://www.ico.gov.uk/>

The NHS Care Records Service

Under the National Programme for Information Technology (NPfIT), the NHS Care Records Service is being introduced over the next few years and this will hold electronic health records in both national and local systems. This is covered by the NHS Care Records Guarantee⁷. Services will include Picture Archiving and Communication Systems, Electronic Prescription Systems, Pathology Messaging etc. All systems and services delivered through NPfIT incorporate stringent security controls and safeguards to prevent unrestricted or uncontrolled access to personal information. An audit trail will be kept of every time a patient NHS Care Record is viewed and edited. Staff should only access patient information when strictly necessary i.e. when they, or their immediate team, are directly involved in the care of that patient. Organisations will run regular comparisons of audit trails with the patients who have attended appointments and Caldicott Guardians will receive automated alerts of irregular activity. Patients will be able to request a copy of their audit trail. Further information is available from NHS Connecting for Health www.connectingforhealth.nhs.uk and reference 18.

Information Governance in IT Systems¹⁹:

- NHS Connecting for Health has developed an Information Governance (IG) toolkit²⁰, which provides information on standards in information governance, guidance, awareness and educational materials, performance measurement tools and support for implementing the standards. Key areas include confidentiality and consent, Data Protection Act, Caldicott standards, information management and technology, security, records management and data accreditation.
- The international standard for information security management is BS ISO/IEC 27002:2005^{20,21}. All information security requirements in the NHS Information Governance Toolkit are based on the standard.
- NHS Connecting for Health has produced an Information Governance Training Tool which contains a range of e-learning modules, trainer materials and a resource library. Further information from:

<http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm>

- NHS Connecting for Health and the BMA have issued a useful document “Joint Guidance on Protecting Electronic Patient Information” which covers personal and organisational responsibilities, including guidance on use of NHSmail for exchanging confidential information, guidance on use of laptops and other mobile devices, use of smartcards, passcodes encryption etc. It emphasises that there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS. The document can be downloaded by BMA members from:

[http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFprotectinginfo/\\$FILE/protecting_patient_info.pdf](http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFprotectinginfo/$FILE/protecting_patient_info.pdf)

The General Medical Council is due to publish further guidance on confidentiality in 2009. This will cover:

- reporting concerns about patients to the DVLA
- disclosing records for financial and administrative purposes
- reporting gunshot and knife wounds
- disclosing information about serious communicable diseases
- disclosing information for insurance, employment, benefit claims and similar purposes
- disclosing information for educational and training purposes
- responding to criticism in the press

1. Standard Statement on Confidentiality Policies

All services should have a written Confidentiality Policy

- 1.1 Service confidentiality policies should be informed by, and updated in line with, latest national guidance, e.g. from the Department of Health ^{1,3,4,5}, General Medical Council ^{6,7} and other professional organisations ^{8,9}.
- 1.2 Service confidentiality policies should be in line with and endorsed by local NHS Trusts.
- 1.3 All staff should sign up to the service's confidentiality policy.
- 1.4 Policies should include guidance on:
 - 1.4.1 handling written, electronic and verbal information ^{1,22}
 - 1.4.2 legal frameworks ** for information sharing as dictated by current guidance ^{1,23,24,25,26,27,28}
 - 1.4.3 sharing information with other NHS services, & non-NHS organisations and agencies in line with current guidance ^{21,22,23}
 - 1.4.4 under 16s ^{7,24}
 - 1.4.5 those unable to give consent ²⁵
 - 1.4.6 avoidance of inadvertent breach of confidentiality ^{1,33,41}
 - 1.4.7 disposal of confidential information ¹⁵
 - 1.4.8 secure storage of paper and electronic records ¹⁵, visual and audio recordings use of email, faxes, SMS etc ^{22,41-46}
 - 1.4.9 client access to paper and electronic records ¹⁸
 - 1.4.10 copying letters to clients ²⁷
 - 1.4.11 safeguarding children / child protection ^{7, 30}
 - 1.4.12 safe transporting and storage of client records both paper-based and electronic) when it is necessary to take them in cars or keep at home, e.g. for domiciliary visits ⁴³
 - 1.4.13 procedure for reporting incidents involving breaches of security or confidentiality ¹
 - 1.4.14 procedures for use of CCTV and recording of telephone calls, publication in print, radio, TV, video, and internet media ⁴¹
 - 1.4.15 disclosure required by statute, disclosure to police, social services and partner organisations, disclosure to solicitors, courts, tribunals and regulatory bodies, disclosure for insurance and occupational health purposes and financial audit, and statutory restrictions on disclosure ⁴¹

- 1.4.16 procedures for secondary uses of information ⁴¹ such as research, epidemiology, public health surveillance, health service planning and education
 - 1.4.17 procedures for handling patient information for teaching, and training, including logbooks and training portfolios
 - 1.4.18 procedures for seeking advice in circumstances when staff are uncertain whether a disclosure without consent is justified
- 1.5 Service users should be involved in the production and implementation of the service's confidentiality policy³⁵

**Particular note should be taken of guidance regarding information on sexually transmitted infections (STIs)²³ using information from screening programmes ²⁴ the Data Protection Act²⁵ rights of access to personal health records^{25,26,27}. Abortion Regulations 1991, reporting of notifiable diseases.

2. Standard Statement on Confidentiality Training

**Services should provide all staff with a programme of
Training on Confidentiality**

- 2.1 Clinical and non-clinical personnel should receive accessible and appropriate training in confidentiality and handling enquiries about sensitive information³³.
- 2.2 All staff should receive training on national Safeguarding Children procedures³⁷, and be able to use local Safeguarding Children policies.
- 2.3 All staff should be trained in the legal requirements of the Data Protection Act^{13, 25, 26} as they apply to health services.
- 2.4 All staff should receive Caldicott training²⁴.
- 2.5 All staff should receive training on the secure use of personally identifiable information in computer systems fax machines, electronic mail, and all forms of portable computing media such as laptops, handhelds, solid state memory cards, USB memory sticks, pen drives, DVDs, CD-ROMs etc^{2,47}
- 2.6 All staff should receive training in confidentiality on taking up employment within the NHS or under contract to an NHS organisation and this training should be regularly updated in line with local Trust policies

3. Standard Statement on Clients Rights to Confidentiality

All clients have the right to expect that information about them will be held in confidence

- 3.1 All services should prominently display their confidentiality statement, which should acknowledge that information will be shared with colleagues within the service in order to provide quality and continuity of care, except in certain well-defined circumstances.
- 3.2 Client literature/service leaflets should contain a statement concerning rights to confidentiality.
- 3.3 Specific permission should be sought from the client regarding the communication to them of test results and any other information²⁷, i.e. whether writing, telephoning, texting or any other means is acceptable to them.
- 3.4 There should be a mechanism for returning undelivered client letters without opening them, e.g. PO Box number.
- 3.5 Specific permission should be sought from the client to sharing any information with anyone outside the service, other than those directly involved in client care, e.g. laboratory staff, except as below**. Information disclosed for secondary uses such as audit, service planning, medical research etc should be anonymised or pseudonymised, but if this is not practicable, the client's express consent should be sought.
- 3.6 With issues relating to safeguarding children / child protection, the client should be informed that sharing will occur.** and the reasons for the disclosure should be given
- 3.7 All staff should be familiar with guidance about the use of photographs and video recordings^{32,41}.
- 3.8 All client records, paper and electronic, should be securely stored and only be accessed on a "need to know / see" basis.
- 3.9 The transfer of written clinical information to other professionals by letter, email or fax should be secure, and clearly marked "In Confidence"
- 3.10 The transfer of clinical information or other personally identifiable information to other professionals by email should be by NHS Mail which uses the secure N3 network and all accounts end in @nhs.net other email accounts that are not encrypted should not be used for this purpose. (<https://www.nhs.net/AcceptableUse.do>)
- 3.11 The Caldicott principles¹⁵ should be applied to all information sharing concerning clients.
- 3.12 No personally identifiable or sensitive information held in electronic format should be transferred across the NHS or to another organisation unless encrypted

** There may be an exception to this when telling a victim of abuse that information will be shared may alert the abuser who could move elsewhere and cause harm to others.

4. Standard Statement on Sharing Non-identifiable Information

Services should ensure that clients are informed that anonymised information may be used for service improvement, audit and clinical

- 4.1 Information used for clinical governance, audit, teaching or other quality improvement purposes should always be anonymised or pseudonymised⁴¹.
- 4.2 Service leaflets should contain a statement concerning the use of anonymised information, including explanation about information from screening programmes^{1,24}. cancer, genetic and disease registers.

5. Standard Statement on Working with Young People

Services should ensure that their staff are aware that all people, irrespective of age, are entitled to the same duty of confidentiality, provided they understand the implications of the advice and treatment offered

- 5.1 All staff should be familiar with the latest Department of Health Guidance on the care of under 16s^{6,31} and guidance from the GMC¹⁰.
- 5.2 All staff working with young people under 16 should be familiar with and use the Fraser Guidelines^{10,31,33,36,38} (or appropriate equivalent guidance^{30,32}) on competence.
- 5.2 All staff working with young people under 18 should be familiar with local and national safe guarding children/child protection guidance and procedures and their impact on confidentiality^{6,37}.

6. Standard Statement on Disposal of Confidential Information

All services should have mechanisms for disposal of confidential information

- 6.1 Services should have clear guidelines for archiving and disposal of old notes²²
- 6.2 All staff should have easy access to shredding for all paper carrying identifiable information (including notes on message pads).
- 6.3 Identifiable audio or electronic information which is no longer required should be permanently deleted.

7. Standard Statement on Disclosure without Consent

Services should inform clients that Personal information should only be disclosed if it is in the public interest, or to protect the individual

Essential (minimum):

- 7.1 All staff and clients should understand that there are exceptional circumstances when confidentiality may not be upheld^{1,9,37,41}. Disclosure may be justified to protect the individual or others to risk of death or serious harm, or be required by law (see Appendix 1)
- 7.2 All staff should be made aware that if they are in any doubt about whether to share information they should seek advice from an experienced colleague, a named or designated doctor for child protection, a Caldicott Guardian, from a professional body, defence organisation or the GMC.

References:

1. Department of Health. NHS Confidentiality Code of Practice 2003
http://www.dh.gov.uk/en/Policyandguidance/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4100550
2. Department of Health. Information Security Management: NHS Code of Practice 2007
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142
3. Joint Guidance on use of IT equipment and access to patient data. DH, GMC and Information Commissioner 2007
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074179
4. Faculty of Sexual & Reproductive Healthcare of the RCOG. Service Standards for Sexual Health Services. January 2006
http://www.ffprhc.org.uk/admin/uploads/814_ServiceStandardsSexualHealthServices.pdf
5. Department of Health. Standards for Better Health. DH 2004 (updated 2006)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4086665
6. Department of Health. You're Welcome quality criteria: making health services young people friendly. DH 2007
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_073586
7. Department of Health. The NHS Care Record Guarantee. DH 2007
http://www.connectingforhealth.nhs.uk/nigb/crsguarantee/crs_guarantee.pdf
8. Department of Health. Connecting for Health: Information Governance: Confidentiality.
<http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/confidentiality>
9. General Medical Council. Guidance on Good Practice – Confidentiality: Protecting and Providing Information. GMC April 2004
http://www.gmc-uk.org/guidance/current/library/confidentiality_faq.asp
10. General Medical Council. 0 – 18 years: guidance for all doctors. GMC 2007
http://www.gmc-uk.org/guidance/current/library/confidentiality_faq.asp
11. United Kingdom Central Council for Nursing, Midwifery and Health Visiting (UKCC). Guidelines for Professional Practice. UKCC1996.
12. Association of Medical Secretaries, Practice Managers, Administrators and Receptionists (AMSPAR). Code of Conduct. AMSPAR 2000.
13. Data Protection Act 1998
14. Freedom of Information Act 2000
15. Department of Health. The Caldicott Committee – Report on the Review of Patient-Identifiable Information. DH 1997. www.dh.gov.uk
16. Department of Health. Implementing the recommendations of the Caldicott Report. HSC1998/089
http://www.dh.gov.uk/en/Publicationsandstatistics/Lettersandcirculars/Healthservicecirculars/DH_4004793
17. The Human Rights Act 1998
<http://www.dca.gov.uk/peoples-rights/human-rights/legislation.htm>

18. Khong S-Y, Currie I, Eccles S. NHS Connecting for Health and National Programme for Information Technology. *The Obstetrician & Gynaecologist* 2008; 10:27-32
19. Information Governance in the Department of Health and the NHS. 2006
<http://www.connectingforhealth.nhs.uk/crdb/boardpapers/igreview/igreview.pdf>
20. Information Governance Toolkit 2008
<https://www.igt.connectingforhealth.nhs.uk/>
21. ISO 17799 / ISO 27001 How to conduct a computer security audit.
http://www.7safe.com/iso27001_iso17799.html
22. Department of Health. Records management: NHS Code of Practice Parts 1 and 2. DH April 2006. Gateway Reference 6295
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747
23. The NHS Trusts and Primary Care Trusts (Sexually Transmitted Disease) Directions 2000 pursuant to Sections 17 and 126(3) of the National Health Service Act 1977(a)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsLegislation/DH_4083027
24. Department of Health. Gateway reference 7019. The Caldicott Guardian Manual.DH2006.
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_062722
25. Department of Health. HSC 2000/009. Data Protection Act 1998: protection and use of patient information
http://www.dh.gov.uk/en/Publicationsandstatistics/Lettersandcirculars/Healthservicecirculars/DH_4002964
26. Department of Health. 2003. Guidance for access to health records requests under the Data Protection Act 1998
http://www.dh.gov.uk/en/Policyandguidance/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084411
27. Access to Health Records Act 1990
http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900023_en_1.htm
28. Department of Health. 2007. NHS Information Governance – guidance on legal and professional obligations. Gateway reference 8523
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_079616
29. Public Sector Data sharing: Guidance on the law. 2003
http://www.justice.gov.uk/docs/data_sharing_legal_guidance.pdf
30. HM Government. 2006. Information sharing vision statement
<http://www.foi.gov.uk/sharing/information-sharing.pdf>
31. Department of Health. Best Practice Guidance for Doctors and other Health Professionals on the Provision of Advice and Treatment to Young People under 16 on Contraception, Sexual and Reproductive Health. July 2004. (Gateway reference number 3382)
32. Department of Health. Reference Guide to Consent for Examination or Treatment.DH2001.
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4006757
33. Royal College of General Practitioners etc Confidentiality and Young People: improving teenagers' uptake of sexual and other health services - A Toolkit for General Practice, Primary Care Groups and Trusts. RCGP and Brook 2000.

34. Department of Health. Copying letters to Patients – Good practice guidelines. DH2003. <http://www.dh.gov.uk/en/Policyandguidance/Organisationpolicy/PatientAndPublicinvolvement/Copyingletterstopatients/index.htm>
35. Royal College of Obstetricians & Gynaecologists. Patient involvement in enhancing service provision – Clinical Governance advice No. 4. RCOG Press 2002
36. Gillick v West Norfolk and Wisbech AHA [1986] AC112, [1985] 3 WLR830, [1985] 3 All ER 402, HL
37. Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children HM Government 2006
www.everychildmatters.gov.uk/files/CCE39E361D6AD840F7EAC9DA47A3D2C_8.pdf
38. Faculty of Sexual & Reproductive Healthcare. Contraceptive Choices for Young People. 2004. <http://www.ffprhc.org.uk/admin/uploads/YoungPeople.pdf>
39. Age of Legal Capacity (Scotland) Act 1991
40. Faculty of Sexual & Reproductive Healthcare. Service Standards on Obtaining Consent in Sexual Health Services. 2007
http://www.ffprhc.org.uk/admin/uploads/949_ServiceStandardsonObtainingValidConsent.pdf
41. BMA: Confidentiality and disclosure of health information toolkit. March 2008
[http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFConfToolKit08/\\$FILE/Confidentiality_Toolkit_2008.pdf](http://www.bma.org.uk/ap.nsf/AttachmentsByTitle/PDFConfToolKit08/$FILE/Confidentiality_Toolkit_2008.pdf)
42. NHSmail Acceptable Use Policy <https://www.nhs.net/AcceptableUse.do>
43. NHS Connecting for Health Home Working procedure 2008
<https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Home%20working%20procedure.doc>
44. NHS Connecting for Health Good Practice in Mobile Computing 2008
<https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Mobile%20computing%20v03.pdf>
45. NHS Connecting for Health: laptop security policy 2008
<https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Exemplar%20Laptop%20Security%20Policy.doc>
46. NHS Connecting for Health: encryption guidance 2008
<https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Encryption%20Guidance%2031.1.2008.doc>
47. NHS Connecting for Health Information Governance Training Tool 2008
<http://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm>

Further reading:

General Medical Council. Good Medical Practice. GMC 2001. www.gmc-uk.org

General Medical Council. Consent: patients and doctors making decisions together GMC 2008
http://www.gmc-uk.org/news/articles/Consent_guidance.pdf

Information for patients/clients:

Private and Confidential – talking to doctors. Brook publications
http://www.brook.org/content/m8_4_confidentiality.asp.

Appendix 1 (from BMA Confidentiality Toolkit 2008⁴¹)

Serious harm and serious crime

Disclosure of information without consent may be justified in the public interest if failure to disclose would expose the client or others to risk of death or serious harm. The NHS Code of Confidentiality suggests that serious harm could be child abuse or neglect, assault, a traffic accident or the spread of a serious communicable disease – which the GMC regards as HIV, tuberculosis, hepatitis B and C. Disclosure without consent may also be justified when disclosure would assist in the prevention, detection or prosecution of serious crime. There is no agreed definition of serious crime but the NHS Code of Confidentiality lists examples as murder, manslaughter, rape, treason, kidnapping, child abuse or neglect and also includes serious harm to the security of the State or public order. The wishes of a competent person to decline consent for disclosure should usually be respected but if their decision exposes others to a risk so serious that it outweighs the client's and the public interest in maintaining confidentiality, information should be disclosed to an appropriate person or authority and the client should be informed of the reasons for the disclosure. Health professionals are expected to participate in procedures set up to protect the public from violent and sex offenders.

Disclosure required by statute

Examples include:

- Notification of diseases under the Public Health (Control of Disease) Act 1984 and Public Health (Infectious Disease) Regulations 1988 – note that the list of notifiable diseases varies within the countries of the UK.
- Abortion Regulations 1991
- Road Traffic Act 1988
- Terrorism Act 2000
- The Information Sharing Index (England) Regulations 2007

Disclosure permitted by statute

Examples include:

- Data Protection Act 1998
- Crime and Disorder Act 1998
- Children Act 1989

Disclosure to solicitors

Health records required for legal proceedings are obtained via the Data Protection Act or Access to Health Records Act 1990. Health professionals should ensure that they have written consent to disclosure and confirm that the client understands the nature and extent of the information disclosed.

Disclosure to courts, tribunals and regulatory bodies

Courts, some tribunals and bodies such as the GMC have legal powers to require disclosure, without the client's consent, of information that may be relevant to matters within their jurisdiction e.g. fitness to practice inquiries. Clients can make representations to the court if they object to disclosure. Health care professionals can apply to the court if they know that the court order requests the release of records that contain information about third parties unconnected with the proceedings.

Statutory restrictions on disclosure

Health professionals are required by law to restrict disclosure of some specific information for example:

- Gender Recognition Act 2004
- NHS (Venereal Diseases) Regulations 1974 and the NHS Trusts and PCTs (Sexually Transmitted Diseases) Directions 2000
- Human Fertilisation and Embryology Act 1990