Service Standards on Confidentiality

October 2015

“Setting standards in contraception - improving sexual health for all”
**Published by the Clinical Standards Committee**

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

**Committee Members:**

Committee members:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair</td>
<td>Dr Jane Dickson</td>
</tr>
<tr>
<td>Vice Chair</td>
<td>Dr Lynne Gilbert</td>
</tr>
<tr>
<td>Members</td>
<td>Dr Paula Briggs</td>
</tr>
<tr>
<td></td>
<td>Dr Dianna Reed</td>
</tr>
<tr>
<td></td>
<td>Dr Helen Munro</td>
</tr>
<tr>
<td></td>
<td>Dr Julianne Lyons</td>
</tr>
<tr>
<td>Revalidation Representative</td>
<td>Dr Louise Massey</td>
</tr>
<tr>
<td>Trainee member</td>
<td>Dr Rachel Westwick</td>
</tr>
<tr>
<td>Nurse Member</td>
<td>Mrs Michelle Jenkins</td>
</tr>
<tr>
<td>Ex-Officio Representatives</td>
<td>Dr Asha Kasliwal</td>
</tr>
<tr>
<td></td>
<td>Dr Ailsa Gebbie</td>
</tr>
<tr>
<td></td>
<td>Dr Alan Tang (BASHH)</td>
</tr>
</tbody>
</table>
Appendix 3

SERVICE STANDARDS ON CONFIDENTIALITY

Published: March 2005
Current Version: October 2015
Review date: October 2018

Changes introduced since review

Clarification of when disclosure of confidential information is allowed, under common law

7th Caldicott principle added

Guidance on identity theft

Guidance on reporting of crimes to police

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 health seeking treatment. They do so in confidence and have the legitimate expectation that staff will respect this trust. All NHS employees are responsible for maintaining and protecting the confidentiality of information relating to patients, which they use in their day to day roles. All identifiable patient information, whether written, computerised, visually or audio recorded or simply held in the memory of health professionals, is subject to the duty of confidentiality.

The Department of Health published “Standards for Better Health” 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.

The Faculty’s Service Standards for Sexual Health Services\(^4\) also includes a standard on confidentiality. 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 and services need to keep up to date with current national policies and guidance.

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, hospital-based settings including community and hospital pharmacies. 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.

**Legal Standards:** There are three areas of law that are most relevant to the processing of patient information\(^5\). These are:

1. **Human Rights Act 1998\(^6\)**

   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 1998**

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. It is based on precedent following other cases. 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.

Under common law, three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented;
- where disclosure is necessary to safeguard the individual,
- or others, or is in the public interest; or where there is a legal duty to do so, for example a court order. ([http://www.dhsspsni.gov.uk/gmgr-annexe-e8](http://www.dhsspsni.gov.uk/gmgr-annexe-e8))
- The Children and Young People Act (Scotland) 2014 is new legislation brought in to practice which states that each child, either pre-school or school age shall have a “named” person, with whom concerns about child protection can be raised. ([http://www.legislation.gov.uk/asp/2014/8/part/4/enacted](http://www.legislation.gov.uk/asp/2014/8/part/4/enacted))

**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 controllers (those who decide how and why personal data are processed). His website 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.org.uk/](http://www.ico.org.uk/) (checked 7.4.15))

The Department of Health’s (DH) key document ‘Confidentiality: NHS Code of Practice’ is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and
patients’ consent to use their health records. A supplementary guidance: Public Interest Disclosures’ expands upon the principles set out within the Code. The document is aimed at aiding staff in making difficult decisions about when disclosures of confidential information may be justified in the public interest.

The Information Security Management: NHS Code of Practice⁹ is a guide to the methods and required standards of practice in the management of information security for those who work within or under contract to, or in business partnership with NHS organisations in England. It is based on current legal requirements, relevant standards and professional best practice.

There has been an update on the policy and practice of sharing patient information relating to sexually transmitted infections obtained in self-referral open-access sexual health services and contraceptive services. Previously, legislation under the NHS Trusts and Primary Care Trusts,(Sexually Transmitted Diseases) Directions 2000 meant that records for the above services were kept separately and shared only with the patient’s consent. Following the Health and Social Care Act 2012, in England, the NHS Trusts and Primary Care Trusts, (Sexually Transmitted Diseases) Directions 2000 apply only to the few remaining NHS hospital trusts and they do not apply to NHS Foundation Trusts or the wider range of services that now provide STI testing and treatment. The 2000 Directions will cease to have effect once the remaining trusts become Foundation Trusts. However, the aim remains unchanged in that people should continue to use self-referral sexual health services with assurance that information on STI testing, diagnosis and treatment will be not be included in their shared patient records without their consent. The department of health is currently working with key stakeholders to explore other existing legislation/law which supports maintaining separate records for people using self-referral sexual health services for STI testing and treatment. The Department of health will then consider the need for further guidance setting out the legal position.

The General Medical Council guidance on confidentiality\textsuperscript{10} is to help doctors identify the relevant legal and ethical considerations, and to help them make decisions that respect patients' privacy, autonomy and choices and that also benefit the wider community of patients and the public. The GMC has also published supplementary guidance on:

- 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

A joint guidance on use of IT equipment and access to patient data has been agreed by the General Medical Council, Information Commissioner and the Department of Health to ensure that all those who have access to patient information in the course of their work are clear about what is expected of them\textsuperscript{5}.

All healthcare professionals must maintain the standards of confidentiality laid down by their professional body\textsuperscript{1,12,2,13} such as the GMC\textsuperscript{10,14}, Nursing and Midwifery Council (NMC)\textsuperscript{11}, General Pharmaceutical Council\textsuperscript{49} 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\textsuperscript{7}. The duty of confidence must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures\textsuperscript{1}.

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\textsuperscript{2,10,44,45}.

Individuals already have the right to access their own personal information under the Data Protection Act, 1998\textsuperscript{7}. The Freedom of Information Act\textsuperscript{15}, 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.

Confidentiality is a Clinical Governance issue – serious breach of confidentiality by NHS employees carries with it severe penalties. The Caldicott principles\textsuperscript{16,17} should always be followed. The 7\textsuperscript{th} principle was added in 2013:

- 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
- the duty to share information can be as important at the duty to protect confidentiality

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”\textsuperscript{13}. 

---

\textsuperscript{1,2,10,12,13,2,10,44,45,7,15,16,17}
NHS Connecting for Health (NHS CFH)\textsuperscript{18,19,20,21,22 23 24,25}

NHS CFH is part of the Department of Health Informatics Directorate. Its role is to maintain and develop the NHS national IT infrastructure. It helps the NHS to deliver new computer services and applications to improve patient care and safety. Some of these include NHS Care Records Service, Information Governance, Choose and Book, Electronic Prescription Service, N3: The National Network, NHS mail\textsuperscript{26}, Picture Archiving and Communications System, Pathology Messaging etc. It has the responsibility of delivering the NHS National Programme for IT (NPfIT), an initiative by the Department of Health to move the National Health Service in England towards a single, centrally-mandated electronic care record for patients and to connect 30,000 General practitioners to 300 hospitals, providing secure and audited access to these records by authorised health professionals.

The NHS Care Records Service

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 (Summary care records held nationally and Detailed care records held locally). The NHS Care Record Guarantee\textsuperscript{27} provides a commitment that the patient’s records will be used in ways that respect their rights to secure, confidential and accurate records. It applies to paper records and to electronic patient records. Stringent security controls and safeguards will 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. Additional safeguards are recommended in general practice settings for children aged 11-16 with respect to proxy access to their care records to prevent inadvertent breaches of confidentiality. elearning.rcgp.org.uk/.../PatientOnline-ProxyAccess-guidance.pdf (accessed 24.6.15)

Care is also required to manage instances of suspected coercion with respect to proxy access to care records for vulnerable individuals.


Information Governance:\textsuperscript{28}

- NHS CFH has developed an Information Governance (IG) toolkit\textsuperscript{19}, 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\textsuperscript{20,21}. All information security requirements in the NHS Information Governance Toolkit are based on the standard.

- NHS CFH has produced an Information Governance Training Tool\textsuperscript{20} which contains a range of e-learning modules, trainer materials and a resource library. Further information from: https://www.igt.hscic.gov.uk (checked 8.4.15)
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. http://systems.hscic.gov.uk/infogov/links/jointguidance.pdf
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 \cite{1,3,5,8,9,16,17,21,29,30,31,32,33,34,35,36,37} General Medical Council \cite{10,14} and other professional organisations \cite{2,4}.

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 or audio information \cite{1,29}.

   1.4.2 Staff to whom the policy applies.

   1.4.2 Legal and professional framework around confidentiality \cite{1,30,31,32,33,34,38,43,44,45}.

   1.4.3 Sharing information with other NHS services, & non-NHS organisations and agencies in line with current guidance, \cite{21,29,30}.

   1.4.4 Under 16s \cite{10,13,35,39,40,41}.

   1.4.5 Those unable to give consent \cite{2,10,32}.

   1.4.6 Avoidance of inadvertent breach of confidentiality \cite{1,2,13,1}.

   1.4.7 Disposal of confidential information \cite{2,29}.

   1.4.8 Secure storage of paper and electronic records \cite{16}, visual and audio recordings use of email, faxes, SMS etc \cite{2,29,25}.

   1.4.9 Client access to paper and electronic records \cite{18,33}.

   1.4.10 Copying letters to clients \cite{27,37}.

   1.4.11 Safeguarding children / child protection \cite{2,10,40}.

   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 \cite{22}.

   1.4.13 Procedure for reporting incidents involving breaches of security or confidentiality \cite{1}.
1.4.14 Procedures for use of CCTV and recording of telephone calls, publication in print, radio, TV, video, and internet media.

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, statutory restrictions on disclosure and disclosure in public interests.

1.4.16 Procedures for secondary uses of information 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, training portfolios and electronic staff records.

1.4.18 Procedures for seeking advice in circumstances when staff are uncertain whether a disclosure without consent is justified.

1.4.19 Information Governance training for staff.

1.4.20 How the implementation of the policy will be monitored, reviewed and compliance assessed.

1.5 Service users should be involved in the production and implementation of the service’s confidentiality policy.

**Particular note should be taken of guidance regarding information on sexually transmitted infections (STIs) using information from screening programmes the Data Protection Act rights of access to personal health records Abortion Regulations 1991, reporting of notifiable diseases. (Note that the list of notifiable diseases varies within the countries of the UK).
2. Standard Statement on Confidentiality training

Services should provide all staff with a programme of training on Confidentiality.

2.1 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. 2.

2.2 Clinical and non-clinical personnel should receive accessible and appropriate training in confidentiality and handling enquiries about sensitive information, including proxy access. 1, 13, 20.

2.3 All staff should receive Caldicott training 31.

2.4 All staff should be trained in the legal requirements of the Data Protection Act 7, 32, 33 and the Freedom of Information Act 2000 15 as they apply to health services.

2.5 All staff should receive training on national Safeguarding Children procedures 40, and be able to use local Safeguarding Children policies.

2.6 All staff should receive Information security training. This should include training on the secure use of personally identifiable information in both paper and electronic record systems, including 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 9, 20.

2.7 Training must be supported by ensuring that staff have ready access to organisational policies, procedures and guidance documents and know where to go for advice when needed 2.
3. **Standard Statement on Clients Rights to Confidentiality**

All clients have the right to expect that information about them will be held in confidence. Patients must be properly informed as to how identifiable information about them is used.

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 information, 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 Explicit consent should be sought for the use or disclosure of personal health information, unless it is clearly implied. 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 When patients withhold consent to disclosure of their information, their wishes should be respected.

3.7 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.

3.8 All staff should be familiar with guidance about the use of photographs and video recordings.

3.9 All client records, paper and electronic, should be securely stored and only be accessed on a “need to know / see” basis.

3.10 The transfer of written clinical information to other professionals by letter, email or fax should be secure, and clearly marked “In Confidence”.

3.11 No personally identifiable or sensitive information held in electronic format should be transferred across the NHS or to another organisation unless encrypted. 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.

3.12 The Caldicott principles should be applied to all information sharing concerning clients.

** 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 Disclosure without Consent**

Confidentiality is not absolute. Services should inform clients that personal information can be disclosed if required by law or in public interests.

4.1 All staff and patients should understand that Confidentiality is an important duty, but it is not absolute. Personal information can be disclosed if:
- it is required by law
- it is justified in the public interest e.g. when child abuse is suspected (see Appendix 1)

4.2 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, a professional body, defence organisation or the GMC.

4.3 The GMC also advises that a disclosure without consent can be justified in the public interest to enable medical research if that research is approved by a Research Ethics Committee. You should alert Research Ethics Committees to disclosures of identifiable information without consent when applying for approval for research projects.

4.4 All staff must document in the patient’s record their reasons for disclosing information without consent and any steps they have taken to seek the patient’s consent, to inform them about the disclosure, or their reasons for not doing so.

4.5

**Medical identity theft** is the illegal access and use of someone's personally identifiable information to fraudulently obtain medical service, prescription drugs or medical insurance coverage. As with general identity theft, the types of information stolen can include name and social security number.

https://oig.hhs.gov/fraud/medical-id-theft/

This can be reported at:
https://www.reportnhsfraud.nhs.uk

4.6 The GMC has some guidance about when a patient’s criminal behaviour can be reported to the police. Disclosure of personal information may be justified in the public interest without a patient’s consent if it would be likely to assist in the prevention, detection or prosecution of serious crime. However, there is no agreed definition of ‘serious crime’, but it would not usually include theft, fraud and damage to property where loss or damage is less substantial.
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 GMC\(^10\) and NICE\(^36\), RCGP

5.2 All staff working with young people under 16 should be familiar with and use the Fraser Guidelines\(^10,31,33,36,41,42\) (or appropriate equivalent guidance) on competence.

5.3 All staff working with young people under 18 should be familiar with local and national safeguarding children/child protection guidance and procedures and their impact on confidentiality\(^6,37,43\).

5.4 Services should use the self-review tool to ensure they meet the Department of Health’s ‘You’re welcome: quality criteria for young people friendly health services’\(^39\). All staff working with young people under 16 should consider if proxy access arrangements to their GP records requires amendment. elearning.rcgp.org.uk/.../0/PatientOnline-Coercion-guidance.pdf (accessed 24.6.15)
6. **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 governance purposes.

6.1 Information used for clinical governance, audit, teaching or other quality improvement purposes should always be anonymised or pseudonymised.

6.2 Service leaflets should contain a statement concerning the use of anonymised information, including explanation about information from screening programmes cancer, genetic and disease registers.
7. **Standard Statement on Disposal of Confidential Information**

All services should have effective mechanisms for disposal of confidential information.

7.1 Services should have clear guidelines for archiving and disposal of old notes.

7.2 All staff should have easy access to shredding for all paper carrying identifiable information (including notes on message pads).

7.3 Identifiable audio or electronic information which is no longer required should be permanently deleted.
References

   

2. BMA: Confidentiality and disclosure of health information toolkit.
   http://bma.org.uk/practical-support-at-work/ethics/confidentiality-tool-kit (accessed 8.4.15)


5. Joint Guidance on use of IT equipment and access to patient data. DH, GMC and Information Commissioner 2007


   http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf (accessed 8.4.15)


14. General Medical Council. 0 – 18 years: guidance for all doctors. GMC 2007
   https://www.igt.connectingforhealth.nhs.uk/
   http://www.gmc-uk.org/static/documents/content/0-18_0510.pdf (accessed 8.4.15)
   Identifiable Information. DH 1997.
   oups/dh_digitallasets/@dh/@en/documents/digitalasset/dh_4068404.pdf (accessed 8.4.15)
   http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/g
   roups/dh_digitallasets/@dh/@en/documents/digitalasset/dh_4011845.pdf (accessed 8.4.15)
   Information Technology. The Obstetrician & Gynaecologist 2008; 10:27-32
20. NHS Connecting for Health Information Governance Training Tool
   https://www.igtt.hscic.gov.uk/igte/index.cfm (accessed 8.4.15)
   http://systems.hscic.gov.uk/infogov/confidentiality (accessed 8.4.15)
22. NHS Home Working procedure 2008 systems.hscic.gov.uk/infogov/igfaqs/homeworking.doc (accessed 8.4.15)
23. NHS Good Practice in Mobile Computing 2008
   https://www.igt.hscic.gov.uk/KnowledgeBase.aspx?tk=419463457957931&lnv=8&cb=b1346440-588f-409d-
   9aa8-7c50a39bd050&isViewOrgType=18&isDesc=Dental+Practice (accessed 8.4.15)
24. NHS laptop security policy 2008
   Documents%2FExemplar%2520Laptop%2520Security%2520Policy.doc (accessed 2008)
25. NHS Connecting for Health: encryption guidance 2008
   https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Encryption%20Guidance
   %2031.1.2008.doc
26. Health and Social Care Information Centre. NHSmail Acceptable Use Policy
   http://systems.hscic.gov.uk/nhsmail/policies (accessed 18.6.15)
27. Health and Social Care Information Centre The NHS Care Record Guarantee. NIGB January 2011
   http://systems.hscic.gov.uk/infogov/confidentiality (accessed 18.6.15)
<table>
<thead>
<tr>
<th></th>
<th>Source</th>
<th>Details</th>
</tr>
</thead>
</table>
| 30.| 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](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsLegislation/DH_4083027)  

40. Working Together to Safeguard Children: A guide to inter-agency working to safeguard and promote the welfare of children HM Government 2010


http://pharmacyregulation.org/standards/standards-registered-pharmacies
Appendix 1 (from BMA: Confidentiality and disclosure of health information toolkit. December 2009)
http://bma.org.uk/practical-support-at-work/ethics/confidentiality-tool-kit

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