NHS Information Governance

Guidance on Legal and Professional Obligations

September 2007

DH INFORMATION READER BOX

Policy HR/Workforce Management Planning Clinical	Estates Performance **IM & T** Finance Partnership working
Document purpose	Best practice guidance
Gateway reference	8523
Title	NHS Information Governance – Guidance on Legal and Professional Obligations
Author	DH/Digital Information Policy
Publication date	September 2007
Target audience	PCT CEs, NHS Trust CEs, SHA CEs, Care Trust CEs, Foundation Trust CEs , Medical Directors, PCT PEC Chairs, NHS Trust Board Chairs, Special HA CEs, Directors of HR, Directors of Finance, Allied Health Professionals, GPs, Royal Colleges, BMA, GMC, Healthcare Commission, Monitor
Circulation list	N/A
Description	The document provides guidance on the range of legal and professional obligations that affect the management, use and disclsoure of information. It will be of particular use to those staff who work in the information governance field.
Cross reference	N/A
Superseded documents	N/A
Action required	N/A
Timing	N/A
Contact details	Liz Waddington Digital Information Policy NHS Connecting for Health liz.waddington@dh.gsi.gov.uk 0113 397 4070
For recipient's use	

Contents

Executive Summary

There is a range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed. This document, which is best practice guidance, outlines the likely impact of these provisions primarily on NHS information but also includes some social care information. Where necessary, organisations should obtain professional legal advice.

The document lists the relevant legal and professional obligations generally in alphabetical order. However, the sections on administrative law and the common law duty of confidentiality have been included at the beginning of Section 1, as they essentially provide a legal background from which much of the legislation has developed. Information governance considerations, to assist those that work in this area, are detailed at the end of each sub-section.

Section 1 Relevant Legislation

1.1 Administrative Law

Administrative law governs the actions of public authorities. According to well-established rules, a public authority must possess the power to carry out what it intends to do. If not, its action is *ultra vires*, ie beyond its lawful powers. It is also necessary that the power is exercised for the purpose for which it was created or is 'reasonably incidental' to the defined purpose.

It is important that all NHS bodies are aware of the extent and limitations of their powers and act *intra vires* (ie within their lawful powers). The approach often adopted by Government to address situations where a disclosure of information is prevented by lack of function (the *ultra vires* rule) is to create, through legislation, new statutory gateways that provide public sector bodies with the appropriate information disclosure function. However, unless such legislation explicitly requires that confidential patient information be disclosed, or provides for common law confidentiality obligations to be set aside, then these obligations must be satisfied prior to information disclosure and use taking place, for example by obtaining explicit patient consent.

Information governance considerations

Staff should be trained in the legal framework covering the disclosure of confidential patient information. They should also be provided with procedures for obtaining explicit consent and guidance on where to seek advice if they are unsure whether they should disclose such information.

1.2 The Common Law Duty of Confidentiality

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges; hence, it is also referred to as 'judge-made' or case law. The law is applied by reference to those previous cases, so common law is also said to be based on precedent.

The general position is that, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the data subject's consent.

In practice, this means that all patient information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient. It is irrelevant how old the patient is or what the state of their mental health is; the duty still applies.

The four sets of circumstances that make disclosure of confidential information lawful are:

- where the individual to whom the information relates has given consent;
- where disclosure is in the overriding public interest;
- where there is a legal duty to do so, for example a court order; and
- where there is a statutory basis that permits disclosure such as approval under Section 60 of the Health and Social Care Act 2001.

Therefore, under common law, a healthcare provider wishing to disclose a patient's personal information to anyone outside the team providing care should first seek the consent of that patient.

Where this is not possible, an organisation may be able to rely on disclosure being in the overriding public interest. However, whether a disclosure is in the public interest is not a decision to be taken lightly. The judgement to be made needs to balance the public interest in disclosure with both the rights of the individual(s) concerned and the public interest in maintaining trust in a confidential service. Solid justification is therefore required to breach confidentiality and specialist or legal advice should be sought before the information is disclosed. Any decision to disclose should be fully documented.

Disclosures required by court order should be referred to the organisation's legal advisers as promptly as possible, so that any necessary representations may be made to the court, for example to limit the information requested.

If a disclosure is made which is not permitted under common law the patient can bring a legal action not only against the organisation but also against the individual responsible for the breach.

Where the disclosure relates to groups of patients rather than individuals, eg for clinical audit or medical research where identifiers are required and consent is genuinely not practicable, then support under Section 60 of the Health and Social Care Act 2001 may be sought through application to the Patient Information Advisory Group.

Information governance considerations

All persons who use patient records should be aware of their responsibility for facilitating and maintaining confidentiality of those records. Systems and processes should ensure that employees only have access to those parts of the record required to carry out their role. Access to records should be logged and periodically audited. Particular care should be taken to protect health records during their transportation between sites or organisations, for example security envelopes and approved carriers should be used where necessary.

Confidentiality: NHS Code of Practice

The Confidentiality Code of Practice is a result of a major public consultation that included patients, carers and citizens, the NHS, other healthcare providers, professional bodies and regulators.

The Code offers detailed guidance on:

- protecting confidential information;
- informing patients about uses of their personal information;
- offering patients appropriate choices about the uses of their personal information; and
- the circumstances in which confidential information may be used or disclosed.

The Code can be accessed from the Department of Health website at: www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf

Disclosure after a patient's death

There are no clear legal obligations of confidentiality that apply to the deceased. Nevertheless, the Department of Health and General Medical Council agree that there is an ethical obligation to the relatives of the deceased in requiring that confidentiality obligations continue to apply.

However, disclosures may be necessary:

- to assist a coroner or other similar officer in connection with an inquest or fatal accident inquiry;
- as part of national confidential enquiries; or
- on death certificates.

Deceased patient records are public records under the Public Records Act 1958. The Information Commissioner's Office has recently published guidance on the matter. This can be found at:
www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/access_to_information_about_deceased_220307_v1.1.pdf

1.3 The Abortion Regulations 1991

These Regulations set out the terms on which certificates of opinion must be issued and held by medical practitioners in order to comply with the Abortion Act 1967. The practitioner who carried out the termination must notify the Chief Medical Officer (CMO) of this fact within seven days of the termination. Under the Regulations, these certificates must be retained by the practitioner who carried out the termination for a period of at least three years.

Information governance considerations

To meet the requirements of these Regulations, organisations must ensure that they have processes in place to ensure that certificates are retained in a secure area for at least three years, and that they are confidentially destroyed once they are no longer required. Disclosure of information to the CMO about terminations does not constitute any breach of confidentiality requirements, as this is a statutory gateway for disclosure

1.4 The Access to Health Records Act 1990

This Act now only affects the health records of deceased patients. It applies only to records created since 1 November 1991.

The Act allows access to:

- the deceased's personal representatives (both executors or administrators) to enable them to carry out their duties; and
- anyone who has a claim resulting from the death.

However, this is not a general right of access, it is a restricted right and the following circumstances could limit the applicant's access:

- if there is evidence that the deceased did not wish for any or part of their information to be disclosed; or
- if disclosure of the information would cause serious harm to the physical or mental health of any person; or

- if disclosure would identify a third party (ie not the patient nor a healthcare professional) who has not consented to that disclosure.

As under the Data Protection Act (DPA) 1998, a medical professional may be required to screen the notes before release.

Under the Act, if the record has not been updated during the 40 days preceding the access request, access must be given within 21 days of the request. Where the record concerns information, all of which was recorded more than 40 days before the application, access must be given within 40 days. However, as with the Data Protection Act 1998, organisations should endeavour to supply the information within 21 days.

A fee of up to £10 may be charged for providing access to information where all of the records were made more than 40 days before the date of the application. No fee may be charged for providing access to information if the records have been amended or added to in the last 40 days.

Where a copy is supplied, a fee not exceeding the cost of making the copy may be charged. The copy charges should be reasonable, as the doctor or organisation may have to justify them. If applicable, the cost of posting the records may also be charged.

Information governance considerations

Although there is no proven duty of confidence owed to deceased patients, the position has yet to be adequately tested in the courts. The Department of Health advises that records of the deceased should be treated as if confidential and disclosures only made in line with the Access to Health Records Act 1990 or other legislation.

Organisations should have processes that address where and how the records of deceased persons are stored. Secure and environmentally safe storage is vital to ensure that records are maintained in good order and are available if required.

It is essential that organisations put in place processes and procedures to enable the efficient and effective retrieval of such records within the timescales specified by the Act.

1.5 The Access to Medical Reports Act 1988

The aim of the Act is to allow individuals to see medical reports written about them, for employment or insurance purposes, by a doctor who they usually see in a 'normal' doctor/patient capacity. This right can be exercised either before or after the report is sent.

The chief medical officer of the employer/insurer is the applicant and he/she will send a request for a report to the doctor. The request must be accompanied by a written and signed patient consent.

The patient may view the report by obtaining a photocopy, or by attending the organisation to read the report without taking a copy away. The patient has a right to view the report from the time it is written and has an opportunity to do so before the report is supplied, or he/she may view it after supply for up to six months.

However, in certain circumstances the patient may be prohibited from viewing all or part of the report if:

- in the opinion of the doctor, viewing the report may cause serious harm to the physical or mental health of the patient; or
- access to the report would disclose third-party information where that third party has not consented to the disclosure.

The patient retains the right to withdraw consent to the report's preparation and/or supply at any time. Therefore, if the patient is unable to view any of the report due to one of the circumstances listed above, he/she can refuse to allow it to be supplied.

If a patient disagrees with the content of the report, he/she has several options. He/she can:

- refuse to allow its supply;
- ask the doctor to correct agreed inaccuracies; or
- have a note added addressing the point(s) of disagreement.

Information governance considerations

Disclosures of medical reports and the information contained within should only take place in accordance with the consent that has been granted by the patient. Disclosures that have not been consented to may be in breach of the common law duty of confidentiality unless they are in line with other statutory considerations.

It is important that these reports remain accessible to the patient for at least six months after they have been supplied to the employer or insurer. After six months, organisations should consider whether retention is necessary; however, if they do decide to retain the report, it must be accessible should a subsequent subject access request be made. In some organisations, it may be easier to hold the report as part of the health record.

1.6 Blood Safety and Quality Legislation

The Blood Safety and Quality Regulations 2005 (amended by the Blood Safety and Quality (Amendment) Regulations 2005 and the Blood Safety and Quality (Amendment) (No. 2) Regulations 2005) implement the provisions of Directive 2002/98/EC (see below) so that the retention periods for data relating to human blood and blood components outlined in the Directive are now part of UK law. The retention periods are as follows:

- Blood establishments must retain certain information regarding donors, establishment activity and testing of donated blood for a minimum of 15 years (regulation 7).
- Blood establishments and hospital blood banks must retain data needed for full traceability for at least 30 years from the point of receipt of the blood or blood component (regulations 8 and 9).

The Regulations also set out requirements for maintaining the confidentiality and security of data (regulation 14) and provide that identifiable information held by blood establishments and blood banks must not be disclosed to third parties unless it is for one of the following reasons:

- to comply with a court order;
- to assist an inspector appointed by the Secretary of State for Health in accordance with these Regulations; or
- to enable tracing of a donation from donor to recipient or from recipient to donor.

Directive 2002/98/EC of the European Parliament and of the Council of 27 January 2003

The Directive sets standards of quality and safety for the collection and testing of human blood and blood components, whatever their intended purpose, and to their processing, storage and distribution when intended for transfusion.

Commission Directive 2005/61/EC of 30 September 2005

The annexes of this Directive set out the data that should be retained for 30 years in order to comply with the traceability requirements of Directive 2002/98/EC.

Data to be retained by blood establishments

Blood establishments should retain:

- blood establishment identification;
- blood donor identification;
- blood unit identification;
- individual blood component identification;
- date of collection (year/month/day); and
- facilities to which blood units or blood components are distributed, or subsequent disposal.

Data to be retained by hospital blood banks

Hospital blood banks should retain:

- blood component supplier identification;
- issued blood component identification;
- transfused recipient identification;
- for blood units not transfused, confirmation of subsequent disposal;
- date of transfusion or disposal (year/month/day); and
- lot number of the component, if relevant.

Information governance considerations

Organisations must ensure that they are able to provide full traceability of whole blood and blood components. There should be a record-keeping system that:

- allows for identification of each single blood donation and each single blood unit and components thereof; and
- enables full traceability to the donor as well as to the transfusion and the recipient.

That is, the method of recording must unmistakably identify each unique donation and type of blood component, the location at which the donation was received and to whom that donation was given.

1.7 The Census (Confidentiality) Act 1991

The Act makes it a criminal offence to unlawfully disclose personal census information.

If the Registrar General, or any person currently or previously employed or contracted to supply services to him, discloses such information they are committing an offence.

If any person further discloses information knowingly acquired by unlawful disclosure, they are committing an offence.

The defences to a charge of unlawful disclosure are that, at the time of the alleged offence, the person believed:

- that he/she was acting with lawful authority; or
- that the information in question was not personal census information and that he/she had no reasonable cause to believe otherwise.

The penalties if convicted are:

- in the magistrates' court, up to six months' imprisonment and/or a fine; or
- in the Crown court, two years' maximum imprisonment and/or a fine.

Information governance considerations

Any staff that may use census information for their work must be instructed on the lawful way in which they may use it and the processes put in place to ensure that unlawful disclosure does not occur.

1.8 The Children Act 2004

This Act, the statutory basis for the Department for Children, Schools and Families Information Sharing Index, places an obligation on NHS bodies to provide information to the Index expressly to enable practitioners dealing with children and young people to share information.

Information governance considerations

Organisations must ensure that staff are adequately trained and put processes in place to ensure that information is appropriately shared.

1.9 The Civil Contingencies Act 2004

This Act and accompanying regulations and non-legislative measures provide a single framework for civil protection in the UK to meet the challenges of the 21st century. The Act is separated into two substantive parts:

- local arrangements for civil protection (Part 1); and
- emergency powers (Part 2).

The overall objective for both parts of the Act is to modernise outdated legislation.

The purpose of Part 1 of the Act is to establish a new statutory framework for civil protection at the local level. This, together with accompanying guidance and regulations, sets out clear expectations and responsibilities for front-line responders at the local level to ensure that they are prepared to deal effectively with the full range of emergencies from localised incidents through to catastrophic events. It divides local responders into two categories.

Those in **Category 1** will have duties placed upon them to:

- assess local risks and use this to inform emergency planning;
- put in place emergency plans;
- put in place business continuity management arrangements;
- put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency;
- share information with other local responders to enhance co-ordination;
- co-operate with other local responders to enhance co-ordination and efficiency; and
- provide advice and assistance to organisations and voluntary organisations about business continuity management (local authorities only).

NHS bodies within **Category 1** include:

- Primary Care Trusts;
- Health Protection Agency;
- NHS Acute Trusts (Hospitals); and
- NHS Foundation Trusts.

Category 2 organisations are placed under the lesser duties of co-operating with Category 1 organisations and for sharing relevant information. These include a range of services and utilities provider organisations.

Information governance considerations

It is important that affected NHS organisations are aware of and comply with their obligations under this Act. These will include the identification of information required to support the organisation's business in the event of an emergency occurring and the development and testing of relevant information technology disaster recovery or fallback continuity plans where computerised information services may be disrupted. However, the Act does not provide a statutory obligation to breach the common law duty of confidentiality. Where information is confidential, the party making the disclosure must consider whether the interests of the individual(s) will be better served by making the disclosure (ie is it in the public interest to disclose?).

1.10 The Civil Evidence Act 1995

This Act provides the legal basis for the use of documents and records of any format to be admissible as evidence in civil proceedings. This includes electronic patient records.

Statements contained within documents may be admissible even where the original document has been lost and only a copy is available.

Documents that form part of a record are also admissible as long as the public authority supplies a signed certificate verifying the authenticity of the document.

Information governance considerations

A public authority is making a legal statement by authenticating such documents and records. The organisation must therefore be sure of the quality and reliability of an electronic record. It will therefore be important to be able to verify that the computer was not misused and was operating properly at the time the record was produced.

1.11 Commission Directive 2003/63/EC (brought into UK law by inclusion in the Medicines for Human Use (Fees and Miscellaneous Amendments) Regulations 2003)

Section 5.2(c) of this Directive gives information about the requirements of marketing authorisation holders regarding retention of documents.

Information governance considerations

Marketing authorisation holders must arrange for essential clinical trial documents (including case report forms) other than the subject's medical files, to be kept by the owners of the data:

- for at least 15 years after completion or discontinuation of the trial; or
- for at least two years after the granting of the last marketing authorisation in the European Community and when there are no pending or contemplated marketing applications in the European Community; or
- for at least two years after formal discontinuation of clinical development of the investigational product.

The subject's medical files should be retained in accordance with applicable legislation and in accordance with the maximum period of time permitted by the hospital, institution or private practice.

The documents can be retained for a longer period, however, if required by the applicable regulatory requirements or by agreement with the sponsor. It is the responsibility of the sponsor to inform the hospital, institution or practice as to when these documents no longer need to be retained.

The sponsor or other owner of the data shall retain all other documentation pertaining to the trial as long as the product is authorised.

The final report shall be retained by the sponsor or subsequent owner, for five years after the medicinal product is no longer authorised.

1.12 The Computer Misuse Act 1990

The Act is relevant to electronic records in that it creates three offences of unlawfully gaining access to computer programs.

The offences are:

- unauthorised access to computer material;
- unauthorised access with intent to commit or cause commission of further offences; and
- unauthorised modification of computer material.

'Access' is defined in the Act as:

- altering or erasing the computer program or data;
- copying or moving the program or data;
- using the program or data; or
- outputting the program or data from the computer in which it is held (whether by having it displayed or in any other manner).

Unlawful access is committed if the individual intentionally gains access; knowing he/she is not entitled to do so; and aware that he/she does not have consent to gain access.

The 'further offence' applies if unauthorised access is carried out with intent to commit or cause an offence.

The 'modification' offence applies if an individual does any act causing unlawful modification of computer material and does so in the knowledge that such modification is unlawful, and with the intent to:

- impair the operation of any computer;
- prevent or hinder access to any program or data held in any computer; or
- impair the operation of any such program or the reliability of any such data.

Future implications and revision to parts of the Computer Misuse Act 1990 are expected when the Police and Justice Act 2006 amendments come into force.

Information governance considerations

It is important that all staff members are aware of and comply with all security measures put in place to protect all health records. The organisation should have policies and procedures in place to facilitate compliance alongside disciplinary measures for failure to comply.

1.13 The Congenital Disabilities (Civil Liability) Act 1976

Where a child is born disabled due to negligent treatment of the mother during pregnancy or childbirth, the child can bring a civil action for damages. This is a separate right to that of the mother. In such a case, the limitation period only begins once the child has reached the age of 18 years. The period may be extended where material facts are not known.

Information governance considerations

Organisations need to take the provisions of this Act into account and ensure that the health records of all children and, in particular, the records of children born with a disability are not destroyed prematurely.

1.14 The Consumer Protection Act (CPA) 1987

This Act allows persons who have suffered damage/injury to themselves or to their private property to make a compensation claim against the manufacturer or supplier of a product. The claimant does not need to prove that the manufacturer/supplier was negligent, merely that it was the product that caused the damage.

The general limitation period in respect of personal injury actions under the Limitation Act 1980 is:

- three years from the date on which the cause of action accrued – so, effectively, the date the accident took place; or
- three years from the date of knowledge that a cause of action had accrued.

When a person dies, the limitation period runs from:

- three years from the date of death; or
- three years from the date when the personal representative had knowledge that a cause of action had accrued, ie the date when they realised that someone was potentially liable for the death.

Section 11A(3) of the Limitation Act 1980 provides that actions in respect of damages for defective products shall not be brought after the expiration of 10 years from the date of supply/manufacture etc, in accordance with the terms of section 4 of the CPA 1987.

Section 11A(4) of the Limitation Act 1980 provides that an action for damages for personal injury caused by a defective product, or loss of, or damage to any property, shall not be later than:

- three years from the date the cause of action accrued; or
- three years from the date of knowledge of the injured person, whichever is the later.

However, it needs to be noted that section 33 of the Limitation Act 1980 provides a discretion to allow an action for damages for personal injury or death to proceed (including damages in respect of personal injury/death caused by a defective

product) if there would otherwise be prejudice to a party to legal proceedings. This discretion does not extend to a claim for loss or damage to property caused by defective products.

Information governance considerations

A claimant generally has three years to begin legal action after the damage; however, this period may be extended to 10 years after the product was supplied. The NHS is affected by these provisions and may be liable as a supplier or user of a product. Therefore, it is important that accurate records are maintained for all products that may fall into this category in order that any claim can be defended.

1.15 The Control of Substances Hazardous to Health (COSHH) Regulations 2002

The COSHH Regulations specify the eight measures that employers must follow to prevent or limit their employees' exposure to hazardous substances.

The measures are:

- assess the risks;
- decide what precautions are needed;
- prevent or adequately control exposure;
- ensure that control measures are used and maintained;
- monitor the exposure;
- carry out appropriate health surveillance;
- prepare plans and procedures to deal with accidents, incidents and emergencies; and
- ensure that employees are properly informed, trained and supervised.

Information governance considerations

The Regulations require that organisations retain records of risk assessments, control measures, exposure monitoring and health surveillance. Some of these records must be kept for specified periods.

1.16 The Copyright, Designs and Patents Act 1990

The Act exists to provide protection for the owners of Intellectual Property Rights (IPR). In broad terms, these are protective rights granted to creators and owners of

works that are the result of human intellectual creativity. These works can be written documents, recordings and include computer software that is considered a literary work.

In general, the objective of IPR is to protect the right of a copyright author in his work and at the same time allow others to access that work. IPR maintain this balance by establishing time limits for the author's control over a particular work. The law that regulates the creation, use and control of the protected work is popularly known as Intellectual Property Law (IP).

The Copyright, Designs and Patents Act 1988 states: 'The owner of the copyright has the exclusive right to copy the work' (section 16). That means it is illegal to copy original works without the copyright owner's permission. With regard to software, the copyright owner is the software developer/publisher. Breaking the law could have serious consequences for an individual and the organisation they work for, threatening both their own and their employer's reputation and future prosperity.

Information governance considerations

It is important that all staff members are aware of and comply with the licensing requirements of software they use, which exist to protect the rights of the software copyright owner. Unauthorised installation, copying, duplication, resale or other misuse of commercial software is likely to breach the terms of licence and could potentially result in criminal prosecution. A copy of the purchase order and licence should be retained for all commercial software purchases.

Corporate web pages where information is published should be checked for infringement of the Act and/or that necessary permissions or acknowledgements have been given. If there is any doubt, check with the organisation's legal advisers.

1.17 The Crime and Disorder Act 1998

The Act provides for Anti-Social Behaviour Orders (ASBOs) to be applied for by a police authority or a local authority against an individual aged 10 years and over. The Anti-social Behaviour Act 2003 amends the 1998 Act to enable a Strategic Health Authority, an NHS Trust or a Primary Care Trust to apply for an ASBO. These can be applied for where that individual has acted in a manner that caused or was likely to cause harassment, alarm or distress to one or more persons not of the same household as him/herself. The function of the Order is the protection of persons in the local government area from further anti-social acts by an individual.

Information governance considerations

Any request for disclosure under this Act must be referred to the Caldicott Guardian and possibly the organisation's legal advisers, who should decide whether such disclosure is necessary or proportionate.

Section 115 of this Act permits the disclosure of personal information that may otherwise be prohibited. There is not a compulsion to disclose and the organisation must make its own decision; however, the requirements of the common law duty of confidence and the Data Protection Act 1998 must still be met. Therefore, information given in confidence must not be disclosed unless there is a clear overriding public interest in doing so.

If a disclosure is to be made, the disclosure must be necessary or appropriate to allow the Crime and Disorder Act 1998 to be applied and the information must only be disclosed to a relevant authority. What is necessary or proportionate depends on the individual circumstances of each case. The outcome to be achieved in disclosing information must be weighed against the public interest in provision of a confidential health service by the NHS.

1.18 The Criminal Appeal Act 1995

Section 17 of the Act gives the Criminal Cases Review Commission powers to demand documents or other materials from public bodies which relate to any case that the Commission is investigating, or any case that relates to a case which they are investigating. The Commission may take any materials away in whatever form it deems appropriate.

Information governance considerations

The exchange of information must comply with the DPA 1998 and sensitive personal data must only be exchanged where the DPA permits.

1.19 The Data Protection Act (DPA) 1998

This Act regulates the processing of personal data, held manually and on computer. It applies to personal information generally, not just to health records. The same principles therefore apply to records of employees held by employers, for example in finance, personnel and occupational health departments.

Personal data is defined as data relating to a living individual that enables him/her to be identified either from that data alone or from that data in conjunction with other information in the data controller's possession. It therefore includes such items

of information as an individual's name, address, age, race, religion, gender and information regarding an individual's physical, mental or sexual health.

Processing includes everything done with that information, ie holding, obtaining, recording, using, disclosure and sharing. 'Using' includes disposal, ie closure of the record, transfer to an archive or destruction of the record.

The Act contains three key strands. These deal with:

- notification by a data controller to the Information Commissioner;
- compliance with the eight data protection principles; and
- observing the rights of data subjects.

Notification by a data controller

The data controller is the person who determines how and why personal information is processed. In practice, for NHS organisations the Trust, Authority or Practice is the data controller. This means that ultimate responsibility for notification will usually rest with the chief executive or GP. The action of notification can be delegated to the most appropriate person within the organisation, for example the head of information management or the information governance lead.

Notification is the process of informing the Information Commissioner of the fact that processing of personal data is being carried out within a particular organisation. Its purpose is to achieve openness and transparency – notification entries are placed in a register so that members of the public can check the type of processing being carried out by a particular organisation. The notification process involves completion of a form stating the name of the data controller and detailing the type of processing being carried out.

Compliance with the eight data protection principles

The **eight principles** advocate fairness and openness in the processing of personal information. The principles state that:

1. Personal data shall be processed fairly and lawfully and must be processed in accordance with at least one of the conditions in schedule 2 of the Act. Where the data being processed is sensitive personal information (such as data relating to the physical or mental health of an individual), it must also be processed in accordance with at least one of the conditions in schedule 3 of the Act.
2. Personal data shall be obtained only for one or more specified and lawful purpose.

3. Personal data shall be adequate, relevant and not excessive for its purpose(s).
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data shall not be kept for longer than is necessary for its purpose(s).
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Information governance considerations

Principle 1

The aim of this principle is to ensure that personal data is processed fairly and lawfully and in accordance with a relevant condition from the schedules to the Act.

To meet the fair processing requirement, individuals must be informed of the fact of processing, including what information will be collected and how it will be held, recorded, used and shared. The Information Commissioner has issued guidance about the meaning of fair processing which indicates that the processing of personal data for purposes other than those for which the data has been provided may be unfair.

To meet the lawful processing requirement, personal data must be processed in accordance with all relevant laws, that is, other statutes such as Article 8 of the European Convention on Human Rights or the common law, such as the duty of confidence.

Health records contain both personal and sensitive data within the terms of the Act; therefore, processing can only be carried out if a condition from both schedules 2 and 3 is met.

The relevant condition to be satisfied for schedule 2 is likely to be one of the following:

- where the processing is necessary for the exercise of any functions conferred on any person by or under any enactment;

- where the processing is necessary for the exercise of any other functions of a public nature exercised in the public by any person;
- where the processing is necessary to protect the vital interests of the patient, ie a 'life or death' situation; or
- with the consent of the patient.

The relevant condition to be satisfied for schedule 3 is likely to be one of the following:

- for medical purposes by a health professional or by a person who owes the same duty of confidentiality as a health professional;
- where the processing is necessary to protect the vital interests of the patient or another person, ie a 'life or death' situation, where consent cannot be obtained or the data controller cannot reasonably be expected to obtain consent;
- where the processing is necessary to protect another person, where consent of the patient has been unreasonably withheld; or
- with the explicit consent of the patient.

Although the Act does not state that explicit consent is required for the processing of health information, compliance with the 'lawful' requirement means that the common law duty of confidence must be taken into account. This duty requires that information given in confidence may not be disclosed without the consent of the giver of that information. Therefore, where health information will be disclosed to someone outside the care team, consent to the processing is necessary (see Section 1.2).

Principle 2

This principle requires that personal data is not processed in a way that is incompatible with the purpose for which it was obtained. Organisations need to specify how they process information in their notification to the Information Commissioner. They are then required to ensure that all processing carried out is in accordance with those stated purposes. Patients should be fully informed about the reason that their information is required, ie they should not be misled into providing information for purposes of which they have no knowledge. If information is obtained for a specific purpose, it must not be used for anything else unless consent is obtained for further uses of the information. For example, identifiable patient information gathered to provide healthcare cannot be used for research unless patient consent is obtained or the information is anonymised. Similarly, employee information collected to enable salary payment should not be

used for purposes unrelated to this, for example marketing of products and services, unless consent is obtained. This principle reinforces the first principle in that it enables patients and the public to find out how a particular organisation states it will use their information.

Principle 3

The aim of this principle is to ensure that organisational records management policies and procedures are in place to support the gathering of relevant, adequate information that is not excessive for its purpose. Organisations should therefore ensure that the information collection procedures in place enable relevant questions to be asked and that training on information collection is made available to all relevant employees.

Systems and processes should be designed to ensure that only relevant information is captured and processed.

The organisation should have procedures in place setting out 'need to know' access controls alongside processes that enable conformance with those controls for each member of staff.

Principle 4

To ensure good data quality, organisations should follow the procedures and processes concerned with information quality in the Information Governance Toolkit. The requirements describe the procedures and processes that organisations should put in place to ensure that information is accurate and kept up to date.

Principle 5

The organisation should have procedures and processes in place for records appraisal so that records are kept for no longer than necessary for the purpose for which they are processed. Organisations should, however, ensure that records are retained for the recommended minimum periods.

The organisation should put in place disposal arrangements for the destruction, archiving and closure of records, and procedures to prevent unnecessary copying of information.

Section 33 and schedule 8, part IV of the Act specifically provide that personal data can be retained for 30 years (or longer) for historical and research purposes. This is reinforced by the further detail given in the Data Protection (Processing of Sensitive Personal Data) Order 2000. GPs currently have an exemption under the Act from

having to delete the records of patients no longer registered. This was negotiated by the Joint GP IT Committee to maintain the integrity of clinical system audit trails, while they are not transferable between clinical systems.

Principle 6

See 'Rights of the individual' below.

Principle 7

Records storage conditions must provide environmentally safe protection for current and archived records.

Records must be protected by effective information security management and records management staff should be aware of and comply with measures put in place. In the guidance issued by the Information Commissioner, certified compliance with BS ISO/IEC 17799:2005 is cited as one of the obvious ways of demonstrating conformance.

Principle 8

This principle is not infringed if the explicit informed consent of the individual is obtained for the transfer. Organisations must ensure that their contract includes terms to cover the protection of the data by the agency to the equivalent of the protection provided by the DPA 1998. In addition, organisations should assess and consider the security management safeguards that will apply at points where data is processed or communicated, and how these will be regularly assured by the contract authority.

Rights of the individual

The DPA 1998 gives an individual several rights in relation to the information held about them.

Of particular relevance in a health and social care setting is the right of individuals to seek access to their records held by the health or social care provider.

Access covers the right to obtain a copy of the record in permanent form, unless the supply of a copy would involve disproportionate effort or the individual agrees that his/her access rights can be met some other way, for example by viewing the record.

Access must be given promptly and in any event within 40 days of receipt of the fee and request. However, the Secretary of State for Health has issued guidance stating

that healthcare organisations should endeavour to meet such requests within a 21-day timescale. This is so that DPA access rights reflect the previous rights contained within the Access to Health Records Act 1990. If the application does not include sufficient details to identify the person making the request, or to locate the information, those details should be sought promptly and the period to respond begins when the details have been supplied.

If access has been given, there is no obligation to give access again until a reasonable period has elapsed. What is reasonable depends on the nature of the data, the purposes for which it is processed and the frequency with which it has been altered.

The right of access is exercisable by the individual:

- making a written application to the organisation holding the records;
- providing such further information as the organisation may require to sufficiently identify the individual; and
- paying the relevant fee.

The fee for providing the individual with a copy of a computerised record is £10. For healthcare records held partially or entirely on paper, the maximum amount that can be charged is £50.

If no permanent record is requested, no fee for access may be made to records that are accessible and contain at least some entries made in the 40-day time period preceding the request, and are not, nor intended to be, automatically processed. A fee of £10 may be charged for viewing records that have not been added to in the 40 days prior to the access request.

There are two main exemptions from the requirement to provide access to personal data in response to a subject access request. These are:

- if the record contains third-party information (ie not about the patient or the treating clinician) where that third party is not a healthcare professional and has not consented to their information being disclosed. If possible, the individual should be provided with access to the part of the record that does not contain the third-party identifier; and
- if access to all or part of the record will seriously harm the physical or mental well-being of the individual or any other person. If possible, the individual should be provided with access to that part of the record that does not pose the risk of serious harm.

Records management staff members have a key role in ensuring that health records can be located, retrieved and supplied in a timely manner. Organisations should ensure that document management structures are set up in such a way as to enable staff members to carry out this role. It is important that system design and operating procedures are established and managed that ensure affected data is accessible where and when required.

1.20 The Data Protection (Processing of Sensitive Personal Data) Order 2000

This Order amends the DPA 1998 and provides that sensitive personal data (for example information relating to physical or mental health) may be lawfully processed without explicit consent where there is a substantial public interest in disclosing the data for any of the following purposes:

- for the detection and prevention of crime;
- for the protection of members of the public against malpractice, incompetence, mismanagement, etc;
- to publicise the fact of malpractice, incompetence, mismanagement, etc, for the protection of the public;
- to provide confidential counselling and advice where explicit consent cannot be given nor reasonably obtained, or where the processing must be carried out without explicit consent so as not to prejudice that confidential counselling or advice; or
- to undertake research that does not support measures or decisions with respect to any particular data subject unless the data subject has explicitly consented and does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

Sensitive personal data may also be lawfully processed where:

- the information relates to the data subject or to specific relatives of the data subject and the processing is for the purposes of administering defined insurance business or occupational pension schemes;
- the processing is carried out by a person authorised under the Registration of Political Parties Act 1998 in the course of their legitimate political business as long as the processing does not cause, nor is likely to cause, substantial damage or substantial distress to the data subject or any other person; or
- the processing is necessary for the exercise of any functions conferred on a constable by any rule of law.

Information governance considerations

The Order amends the DPA 1998 by defining several circumstances under which it would be lawful to disclose sensitive personal data without explicit consent. However, there must be a substantial public interest in making the disclosure; therefore, any decision must involve the Caldicott Guardian and may require referral to the organisation's legal advisers.

1.21 The Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005

These Regulations require that adoption agencies keep records on the adopted children they have placed for at least 100 years and place limits on the information that can be disclosed.

Information governance considerations

The Regulations require that adoption agencies keep records on the adopted children they have placed for at least 100 years and place limits on the information that can be disclosed.

1.22 The Electronic Commerce (EC Directive) Regulations 2002

The key features of these Regulations are:

- online selling and advertising is subject to the laws of the UK if the trader is established in the UK. Online services provided from other EU member states may not be restricted. There are exceptions, particularly for contracts with consumers and the freedom of parties to choose the applicable law;
- recipients of online services must be given clearly defined information about the trader, the nature of commercial communications (ie emails) and how to complete an online transaction;
- online service providers are exempt from liability for the content that they convey or store in specified circumstances; and
- changes to the powers of enforcement authorities such as Trading Standards Departments and the Office of Fair Trading.

Organisations that conduct business online should also be aware of the requirements placed on them by the Distance Selling Regulations 2000, which implemented Distance Selling Directive 97/7/EC of 20 May 1997, on the protection of consumers in respect of distant contracts.

The purpose of the Directive (and therefore the Regulations) is to ensure the free movement of 'information society services' across the European Union; to encourage greater use of e-commerce by breaking down barriers across Europe; and to boost consumer confidence and trust by clarifying the rights and obligations of organisations and consumers.

The E-Commerce Directive was adopted on 8 June 2000 and published in the *Official Journal of the European Communities* on 17 July 2000. The objective was to ensure that information society services benefit from the internal market principles of free movement of services and freedom of establishment, in particular through the principle that they can trade throughout the European Union unrestricted, or what is known as the 'country of origin' rule.

Information governance considerations

While NHS organisations may not currently offer online selling services of this type, it is possible that these may arise in future, or that staff of NHS organisations may participate in online transactions provided by external organisations. Many NHS organisations have already implemented websites to promote their corporate identity and services. Organisations need to consider the potential implications of these Regulations when designing new NHS online services.

1.23 The Electronic Communications Act 2000

The purpose of the Act is to increase confidence in electronic transactions by providing:

- legal admissibility for digital signatures;
- registration of cryptography service providers; and
- repeal of and amendments to legislation that places limits on electronic communication and electronic storage of information.

The Act refers to cryptographic service providers who may employ Public Key Infrastructure (PKI) technology. This technology can be used to limit access to information to those authorised to access it (via a private key), provide a legal basis for the use of digital signatures to verify the identity of the sender and/or authenticate digital access credentials.

Information governance considerations

Organisations should ensure that electronic information is held and transferred in accordance with the Act and other provisions, to ensure that confidential information is accessed only by those with a need to know it in order to carry out their role. They should do their best to ensure that electronic signatures can be verified in case the authenticity of a signature becomes subject to a legal dispute.

Organisations should also be aware of the need to ensure the retention and protection of any cryptographic keys that have been used to protect records, as they may have evidential value over the lifetime of the record.

1.24 The Environmental Information Regulations (EIR) 2004

The Environmental Information Regulations 2004 came into force at the same time as the Freedom of Information (FOI) Act 2000 and update and extend previous rights to environmental information.

Any request for information held by/on behalf of a public authority is initially treated as an FOI request. However, section 39 of the FOI Act 2000 exempts environmental information from being dealt with under FOI and provides for it to be dealt with under EIR 2004. This means that there may be cases where information is exempt under FOI but has to be released under these Regulations. (Where there is a conflict between EU regulations and UK legislation, the EU law takes precedence.)

The Regulations are very similar to the FOI Act 2000 and requests for environmental information are dealt with in a similar way to those for other information. The key differences between EIR 2004 and the FOI Act 2000 are:

- a wider range of organisations are covered by the EIR 2004, including some private organisations;
- the EIR 2004 relate to environmental information only;
- requests for information do not have to be in writing under the EIR 2004 – they can be verbal; and
- all exemptions for refusing an EIR 2004 request are subject to a public interest test.

Personal information of the applicant continues to be dealt with under data protection legislation.

Information governance considerations

As with the FOI Act 2000, the organisation needs a robust records management programme. The requirements of the two pieces of legislation are similar so it is advised that organisations deal with requests in a like manner. The main difference is that requests for environmental information need not be in writing.

1.25 The Freedom of Information (FOI) Act 2000

The FOI Act lays down requirements for the public bodies listed in schedule 1 (including the NHS) to keep and make information available on request.

Designating private organisations as public authorities

If an organisation doesn't meet the conditions for inclusion in schedule 1, section 5 of the Act gives the Secretary of State the power to designate private organisations as public authorities if either:

- they appear to be performing functions of a public nature; or
- they are carrying out functions under contract with a public authority which would otherwise be up to the authority to provide.

No designations have been made yet.

Private companies need to be aware of the effect of the FOI Act 2000 when contracting with public authorities. Information given to the public authority by the private company is effectively 'held by the public authority' and is therefore potentially accessible under the Act. This could include contracts and other documents that the private company considers is commercially sensitive. In some circumstances, the private company may legitimately require that access to information it has provided, eg trade secrets, is restricted or withheld. However, the private company should also be aware that the exemption within the Act for commercially sensitive information (section 43) is a qualified exemption. This means it is subject to a public interest test; therefore, if information is requested which purports to fall within section 43, the public authority should only refuse to provide the information if it believes the public interest in withholding the information outweighs the public interest in disclosing it.

The new rights of access in the FOI Act 2000 signal a new recognition of, and commitment to, the public interest in openness about government. They are additional to other access rights, such as access to personal information under the DPA 1998 and access to environmental information under the EIR 2004.

The main features of the FOI Act 2000 are:

- a general right of access to recorded information held by public authorities, regardless of the age of the record/document; and
- a duty on every public authority to adopt and maintain a scheme that relates to the publication of information by the authority and is approved by the Information Commissioner.

Section 46 of the Act placed a duty on the Lord Chancellor to issue a Code of Practice on records management. The Code has been published and although compliance is not obligatory, it provides guidance to all public authorities as to the practice which it would, in the opinion of the Lord Chancellor, be desirable for them to follow in connection with the discharge of their functions under the FOI Act 2000. Additionally, the Code will be used by the Information Commissioner when deciding whether a public authority has properly dealt with a case (in the event of a complaint).

General right of access

The Act confers two rights on the general public:

- the right to be informed whether a public body holds certain information; and
- the right to obtain a copy of that information.

However, the Act recognises that there can be valid grounds for withholding information and provides a number of exemptions from the right to know, some of which are absolute exemptions and some of which are subject to a public interest test.

As regards exemptions subject to the public interest test, organisations must weigh up whether the public interest in maintaining the exemption in question outweighs the public interest in disclosure.

The request for information must:

- be in writing;
- state the name of the applicant and an address for correspondence; and
- describe the information requested.

The applicant can request that information be communicated by:

- a copy in permanent form (or other form acceptable to them, for example on CD-ROM or audio tape);
- inspection of records; or
- a summary or digest of the information held.

Organisations may charge a fee for reasonably incurred costs to:

- inform the applicant whether it holds the information; and
- communicate the information to the applicant.

However, they are not obliged to charge a fee, and the Ministry of Justice suggests that the fee should be waived where the costs incurred are minimal. If a fee is required, this should be notified to the applicant and paid within three months of receipt of the notice, otherwise the public authority need not comply with the request.

A fee may be charged to cover:

- the cost of putting the information into the applicant's requested format, for example CD, or audio tape;
- photocopying and printing costs (set at no more than 10 pence per page); and
- postage or other transmission costs.

In calculating the cost, organisations are not permitted to take account of employee time required to carry out the work. Additionally, organisations may not charge for putting the information into another format if they are already under a duty to make information accessible under other legislation, for example the Disability Discrimination Act (DDA) 1995.

There may be a few cases where the costs of meeting a request would exceed the appropriate limit, set at £450 (or £600 for central government). If this is the case, organisations are allowed to refuse to answer the request.

The time for compliance by the public authority is the 20th working day following receipt of the request or further information and/or the appropriate fee. This period can be altered by the Secretary of State (up to the 60th working day).

A public authority need not comply with vexatious requests and repeated requests for information already supplied, unless a reasonable period has elapsed between requests.

Publication scheme

A publication scheme should be a complete guide to the information routinely published by an organisation. It is a description of the information about the organisation which is made publicly available and which should act as a route map so that the public can easily find information about the organisation.

The publication scheme must specify:

- the classes of information published, or intended to be published;
- the manner in which publication is, or is intended to be, made; and
- whether the information is available free of charge or whether payment is required.

Information governance considerations

The organisation should carry out a records audit to determine what records it holds, the location of the records and whether they need to be kept. This should lead to a review of the organisation's retention schedules and provide information for its publication scheme.

As with DPA 1998 subject access requests, appropriately trained staff and effective procedures are crucial to compliance with this Act. There is a duty imposed on organisations to supply information in a timely fashion – currently within 20 working days. To facilitate this obligation to provide information within these time limits, the organisation must ensure that all employees are aware of how an FOI Act 2000 application should be progressed and of the requirement to respond to requests quickly.

Organisations should consider maintaining a log of requests with the view to making frequently requested information available through the publication scheme.

1.26 The Gender Recognition Act 2004

The Act gives transsexual people the legal right to live in their acquired gender. It established the Gender Recognition Panel, which has the authority to issue a Gender Recognition Certificate. Applicants to the Gender Recognition Panel are required to supply evidence from a medical practitioner in support of their application. Issue of a full certificate provides legal recognition of a transsexual person's acquired gender.

Under the Act, information relating to an application for a Gender Recognition Certificate is 'protected information', if it is acquired in a professional capacity. It is an offence to disclose protected information to any other person unless an exemption applies. Some of the exemptions are:

- the person has consented;
- the person cannot be identified from the information;
- information is needed for the prevention and investigation of crime;
- information is needed to comply with a court order.

Information governance considerations

As protected information covers all information that would identify a person as being a transsexual, if an applicant is successful in their application a new health record must be created so that protected information is not disclosed.

1.27 The Gender Recognition (Disclosure of Information) (England, Wales and Northern Ireland) (No. 2) Order 2005

It is not an offence to disclose the protected information referred to under the Gender Recognition Act 2004 if:

- the disclosure is made for medical purposes to a health professional; and
- the person making the disclosure reasonably believes that the subject has given consent to the disclosure or cannot give such consent.

'Medical purposes' includes the purposes of preventative medicine, medical diagnosis and the provision of care and treatment.

Information governance considerations

The Order defines the circumstances under which it would be lawful to disclose protected information. Staff should be appropriately trained in seeking informed consent. Where consent cannot be given, a decision to disclose must be taken by senior personnel only.

1.28 The Health and Safety at Work etc Act 1974

The Act imposes duties on employers to look after the health and safety of their employees, and responsibilities on employees to comply with the measures put in place for their health and safety.

There are also six sets of regulations concerned with health and safety at work:

- Management of Health and Safety at Work Regulations 1999;
- Workplace (Health, Safety and Welfare) Regulations 1992;
- Display Screen Equipment Regulations 1992;
- Provision and Use of Work Equipment Regulations 1992;
- Manual Handling Regulations 1992; and
- Personal Protective Equipment Regulations 1992.

These regulations require that employers carry out risk assessments and provide employees with information and training where necessary.

The Management of Health and Safety at Work Regulations 1999 set out more explicitly what organisations must do to comply with the Health and Safety at Work etc Act 1974. The Health and Safety Executive has published an approved Code of Practice for use with the Regulations. The Code has special legal status – a court will take account of whether an organisation has followed the Code in prosecutions for breach of health and safety legislation, unless the organisation can prove that they complied with the law in some other way.

Information governance considerations

Organisations should retain equipment maintenance records, records of assessments and training records etc for appropriate periods, as proof that they are complying with the law and maintaining the safety of their employees. Retention of these records will also assist organisations to appropriately defend against any legal action and comply with investigations carried out by the Health and Safety Executive and/or the Healthcare Commission.

1.29 The Human Fertilisation and Embryology Act 1990, as amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 1992

The Act is retrospective and applies to information obtained before and after it was passed.

The Act prohibits the disclosure by current and former members and employees of the Human Fertilisation and Embryology Authority of:

- any information contained within the Authority's register; and

- any information obtained with the expectation that it would be held in confidence.

The Human Fertilisation and Embryology Authority (Disclosure of Donor Information) Regulations 2004 (SI 1511) prescribe the information that the Authority will provide to persons who have attained the age of 18 and who may have been born in consequence of treatment services under the Act.

The Government is conducting a review of the whole of this Act and will be holding a public consultation on many aspects of it. This review will include consideration of the confidentiality provisions of the Act, and their compatibility with the FOI Act and the DPA.

Information governance considerations

To meet the requirements of this Act, organisations must ensure that they have processes in place to ensure that such information is available only to those permitted access. This is especially important as regards paper records, where information on this form of treatment is likely to be included within past medical history (particularly hospital records).

1.30 The Human Rights Act 1998

This Act became part of UK law on 2 October 2000. It does not contain new rights. It incorporates the European Convention on Human Rights into UK law, allowing an individual to assert their Convention rights in UK courts and tribunals, rather than at the European Court in Strasbourg.

The Convention rights can be sought only against a public body, including NHS and social care organisations. Article 8 of the Convention – the right to respect for private and family life – is the most relevant to information governance issues.

The right to respect for private and family life contains four rights. These are:

- the right to respect for private life;
- the right to respect for family life;
- the right to respect for one's home; and
- the right to respect for correspondence.

Article 8 is not an absolute right, in that the Convention makes provision for interference with the rights (see below). It does, however, impact on subject access requests, consent, confidentiality and disclosure issues.

The right to respect for private life

The current approach is that the right to respect for private life includes an obligation on a public body to meet subject access requests. Denial of access could be interpreted as a breach of Article 8 as it prevents an individual gaining access to information held about him/her. This reflects the rights of the individual under the DPA 1998. Legislation must be read, as far as possible, in a way that is compatible with the Convention.

The right to respect for private life can also be invoked where treatment information is withheld from the individual. If an individual consents to treatment but has not been given sufficient information to make a fully informed decision, that consent will not be valid. Arguably, the withholding of information is a breach of the Article 8 right.

The Article 8 right reflects the common law duty of confidentiality in that patient information should only be disclosed with that patient's consent. If information is inappropriately disclosed, the individual can take legal action for breach against the public body concerned.

Not only must patient information be held confidentially, it must also be held securely. Failure to do so will also breach the right to respect for private life.

The right to respect for family life

This right may also be relevant, in that relatives of the ill often wish to be involved in the decision-making process and kept informed of progress. However, this right must be balanced against the patient's right to confidentiality.

The right to respect for family life becomes even more relevant where the patient is a child or 'incompetent' adult. Failure to keep the family informed can be seen as an interference with this right, actionable under the Act. However, in a situation where the child is 'competent' and does not wish for information to be shared with their family, the young person's right to confidentiality is likely to outweigh the right of the family.

Explaining this may bring the professional into conflict with the family, but ultimately the right of the individual to have information held confidentially will outweigh the right of the family to be kept informed.

It may be possible to claim that one's rights in relation to respect for family life have been breached in an employment context. An employee with an excessive workload, such that it impinges on his/her life outside of the work environment, could possibly plead interference with his/her right to respect for family life.

The right to respect for correspondence

Correspondence includes written and telephone communications. It may be relevant for an individual to assert this right in relation to the monitoring of workplace emails, in particular, if the employee has not been informed that he/she 'has no reasonable expectation of privacy' and that workplace monitoring is taking place. To lessen the risk of being sued under this right, an employer should ensure that:

- the organisation complies with the advice from the Information Commissioner;
- all employees are informed of the organisational policy on 'private' emails (which should also include the use of the telephone and internet); and
- consistent decisions are taken if policy breaches are discovered.

Interference with an Article 8 right

Article 8 rights are qualified rights. This means that in certain circumstances they can be set aside by the state. However, this interference must be lawful, for a legitimate social aim and necessary to achieve that aim. Furthermore, the interference must not be disproportionate to the objective to be achieved.

Legitimate social aims are:

- national security;
- protection of public safety;
- protection of health or morals;
- prevention of crime or disorder;
- protection of the economic well-being of the country; and
- protection of the rights and freedoms of others.

The public body will have to weigh up the public interest necessity of breaching an Article 8 right against the rights of the individual.

Information governance considerations

Current understanding is that if organisations comply with the provisions of the common law duty of confidence and the DPA 1998 they will meet the requirements of Article 8.

1.31 The Limitation Act 1980

This Act sets out the law on the time limits within which actions for personal injuries, or arising from death, may be brought. The limitation period for bringing such actions is three years. This period runs from the date of personal injury or death, or the date when it is first realised that a person has suffered a significant injury that may be attributable to the negligence of a third party.

The Congenital Disabilities (Civil Liability) Act 1976 (see page 14) clarifies the right of a child born disabled, as distinct from the right of his/her mother, to bring civil action for damages in respect of that disability. For a minor, the limitation period runs from the time he/she attains the age of 18 years and may be extended where material facts are not known.

A person of 'unsound mind', as long as he remains under the disability in question, can bring an action without limit of time through his 'next friend'. After the person's death, the period of limitation will run against his personal representative(s). Discharge from hospital does not imply that the person has fully recovered from the disability.

The limitation period of three years from the date of personal injury or death, or date of knowledge of a claim, applies only to actions that include a claim for damages in respect of personal injuries. In the case of other claims, for example a claim by a mentally disordered patient that he has been falsely imprisoned, the appropriate limitation period prescribed by section 2(1) of the Limitation Act 1980 is six years from the date when the patient ceases to be under a disability or dies.

For the purposes of the Limitation Act, a person of 'unsound mind' is a person who, because of mental disorder within the meaning of the Mental Health Act 1983, is incapable of managing and administering his property and affairs. This definition is consistent with the definition of 'disability' in the Supreme Court rules that prescribe how people under a disability may bring an action.

Information governance considerations

A claimant generally has three years to begin legal action after an injury. However, the lapse between an 'injury' and 'knowledge' of it is without limit of time. Therefore, it is important that accurate records are retained in accordance with national guidance and local policies. As with other statutory provisions, organisations must be able to locate and supply information if requested and ensure that closed records are stored in accordance with National Archives' guidance.

1.32 The Medicines for Human Use (Clinical Trials) Amendment Regulations 2006

Sections 18 and 28 of these Regulations give information on the trial master file and archiving, and the requirements of ethics committees to retain documents.

Information governance considerations

The sponsor and the chief investigator shall ensure that the documents contained, or which have been contained, in the trial master file are retained for five years after the conclusion of the trial.

The sponsor and the chief investigator shall ensure that the medical files of trial subjects are retained for at least five years after the conclusion of the trial.

An ethics committee shall retain all the documents relating to a clinical trial on which it gives an opinion for:

- where the trial proceeds, at least three years from the conclusion of the trial; or
- where the trial does not proceed, at least three years from the date of the opinion.

1.33 The National Health Service Act 2006

Section 251 of the National Health Service Act 2006 provides the power to ensure that patient-identifiable information needed to support essential NHS activity can be used without the consent of patients. The power can only be used to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice. It is intended largely as a transitional measure while consent or anonymisation procedures are developed, and this is reinforced by the need to review each use of the power annually.

Section 252 provides for the continuation of a statutory committee – the Patient Information Advisory Group (PIAG). The Secretary of State for Health is required to consult with PIAG before making any regulations under section 251.

Interested persons, for example researchers or database holders, are required to seek permission from PIAG to enable the lawful processing of patient information where it is not possible to obtain consent. Permission is not automatically granted. The applicant must show that their application will improve patient care or is in the public interest, and detail why they are unable to either gain consent or use anonymised information instead.

Information governance considerations

Procedures should be put in place to provide information under section 251 regulations. Organisations should also have a process to inform anyone requesting patient-identifiable information for purposes other than direct healthcare of the need to gain approval from PIAG, unless they have the explicit consent of the patient.

1.34 The NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000

Section 2 of these Directions repealed regulation 2 of the National Health Service (Venereal Diseases) Directions 1991 and annex B, part 1 of the National Health Service Trusts (Venereal Diseases) Directions 1991.

The National Health Service (Venereal Diseases) Regulations 1974 (SI 1974/29) imposed on health authorities an obligation to ensure that information about sexually transmitted diseases obtained by their officers should be treated as confidential. In 1991, Directions were made imposing the same obligation on trustees and employees of an NHS Trust.

These new Directions, which apply only to England, impose the same obligations of confidentiality on the members and employees of both NHS Trusts and Primary Care Trusts (PCTs).

Every NHS Trust and PCT must take all necessary steps to ensure that any information capable of identifying an individual obtained by any of their members or employees with respect to persons examined or treated for any sexually transmitted disease shall not be disclosed except:

- for the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof; and
- for the purpose of such treatment or prevention.

Information governance considerations

To meet the requirements of this Act, organisations must ensure that they have processes in place to ensure that such information is available only to those permitted access. This is especially important as regards paper records, where information on this form of treatment might be included within past medical history (particularly hospital records).

Every NHS Trust and PCT must take all necessary steps to ensure that any information capable of identifying an individual obtained by any of their members or employees with respect to persons examined or treated for any sexually transmitted disease shall not be disclosed except:

- for the purpose of communicating that information to a medical practitioner, or to a person employed under the direction of a medical practitioner in connection with the treatment of persons suffering from such disease or the prevention of the spread thereof; and
- for the purpose of such treatment or prevention.

1.35 The Police and Criminal Evidence (PACE) Act 1984

Under section 69 of this Act, a statement in a document produced by a computer is not admissible as evidence in criminal legal proceedings unless it can be shown that:

- there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer; and
- at all times the computer was operating properly or, if not, that any respect in which it was not operating properly or was out of operation did not affect the production of the document or the accuracy of its contents.

Therefore, before a judge can decide whether computer print-outs are admissible as evidence, it will be necessary to call appropriate authoritative evidence to describe the function and operation of the computer. This is normally a statement of evidence as to how the print-out was obtained. A certificate signed by a person occupying a responsible position in relation to the operation of the computer will also be required. That person must state that the computer system was operating correctly at the time the evidence was obtained.

Information governance considerations

Those responsible for managing any computer system from which information is requested which is to be used as evidence should be aware that they will need to provide a statement that the computer was operating properly at the time that the evidence was provided, or that any malfunction did not affect the production or accuracy of the document. They may also be requested to provide information on the function and operation of the system.

1.36 The Privacy and Electronic Communications (EC Directive) Regulations 2003

These Regulations revoke the Telecommunications (Data Protection and Privacy) Regulations 1999 and are concerned with the processing of personal information and the protection of privacy in the electronic communications sector.

The Regulations set out:

- circumstances under which direct marketing may be carried out;
- duties to safeguard the security of a communications network service;
- limitations on what may be stored or accessed; and
- restrictions on the processing of traffic and location data.

The Regulations are enforced by the Information Commissioner.

Website cookies

The use of cookies on websites is clarified, such that they can be used so long as website visitors are provided with 'clear and comprehensive' information on the information collected and how it will be used, and are given the opportunity to refuse the storage of, or access to, the information.

Information governance considerations

Staff with responsibility for information security management should be aware of the Regulations and their potential implications for the technical design of NHS websites. Consideration is also necessary for the use of email within NHS business activities and in particular the rules for unsolicited email marketing.

1.37 The Public Health (Control of Diseases) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988

Under this legislation, doctors in England and Wales have a statutory duty to notify a 'Proper Officer' of the local authority if they are aware that, or have cause to suspect that, a patient is suffering from one of the notifiable diseases. The doctor must complete a certificate stating:

- the name, age and sex of the patient and the address of the premises where the patient is residing;
- the notifiable condition from which the patient is, or is suspected to be, suffering;

- the date, or approximate date, of the onset of the condition; and
- if the premises are a hospital, the day on which the patient was admitted, the address of the premises from which he/she came there and whether or not, in the opinion of the person giving the certificate, the condition from which the patient is, or is suspected to be, suffering was contracted in hospital.

The list of notifiable diseases can be found on the Health Protection Agency's website at: www.hpa.org.uk/infections/topics_az/noids/noidlist.htm.

Information governance considerations

Organisations should ensure that copies of the notification certificate or counterfoils from a notification book are held securely and retained for the recommended minimum period.

Doctors must complete a certificate stating:

- the name, age and sex of the patient and the address of the premises where the patient is residing;
- the notifiable condition from which the patient is, or is suspected to be, suffering;
- the date, or approximate date, of the onset of the condition; and
- if the premises are a hospital, the day on which the patient was admitted, the address of the premises from which he/she came there and whether or not, in the opinion of the person giving the certificate, the condition from which the patient is, or is suspected to be, suffering was contracted in hospital.

1.38 The Public Interest Disclosure Act 1998

This Act allows a worker to breach his duty as regards confidentiality towards his employer for the purpose of 'whistle blowing'. A disclosure qualifying for protection under the Act is known as a 'qualifying disclosure'.

Such a disclosure is allowed in the following circumstances:

- where criminal activity or breach of civil law has occurred, is occurring or is likely to occur;
- where a miscarriage of justice has occurred, is occurring or is likely to occur;
- where health and safety has been, is being or is likely to be compromised;
- where the environment has been, is being or is likely to be damaged; or

- where information indicating evidence of one of the above circumstances is being or is likely to be deliberately concealed.

It makes no difference whether the circumstances leading to the breach occur within or outside of the UK, as long as either UK law or the law of the other jurisdiction prohibits them.

A qualifying disclosure must only be made:

- in good faith to the individual's employer, or to any other person having legal responsibility for the conduct complained of;
- for the purpose of obtaining legal advice;
- where the worker is employed by the Crown, in good faith to a Minister of the Crown; or
- in good faith to a person prescribed by the Secretary of State.

Under this Act, the worker must reasonably believe that any allegation he makes is substantially true.

If it is the employer who is responsible for the conduct complained of, the Act allows a worker to make a disclosure to a person not noted above, provided the following conditions are met:

- it must be made in good faith, and not for personal gain, with a reasonable belief that the allegations complained of are true; and
- the worker reasonably believes that he will suffer a detriment if he makes the disclosure to his employer; or
- he has previously complained of the conduct and no action has been taken; or
- he reasonably believes that evidence of the conduct has been or will be destroyed or concealed.

Such a disclosure will be subject to a test of reasonableness, which is tested with reference to:

- the person the disclosure was made to;
- the seriousness of the conduct complained of;
- whether the conduct is continuing;
- whether any previously made complaint was acted upon; and
- whether the worker followed any procedure laid down by the employer.

Information governance considerations

Staff should be made aware of the correct procedures to be followed if circumstances arise that require them to breach confidentiality and any policy guidance; see Health Service Circular (HSC) 1999/198 on public interest disclosure.

1.39 The Public Records Act 1958

All NHS records, and those of NHS predecessor bodies, are public records under the terms of the Public Records Act 1958. The Act sets out broad responsibilities for everyone who works with such records and provides for guidance and supervision by the Keeper of Public Records. It requires that those records that have been selected for archival preservation are transferred to the National Archives or a 'Place of Deposit' appointed under the Act.

The maximum period for which records can be kept prior to transfer is usually 30 years. (Any NHS body that feels it needs to hold records for a longer period must consult with the National Archives.) In practice, NHS records that have been selected for archival preservation are transferred to a Place of Deposit which is usually the record office of the relevant local (ie county, borough or unitary) authority. Some individual hospitals have been appointed as a Place of Deposit, although these have tended to be those larger hospitals that can commit the resources necessary to provide appropriate conditions of storage and access and to place them under the care of a professionally qualified archivist.

Information governance considerations

Further guidance is given in the introduction to the retention schedules in *Records Management: NHS Code of Practice*, available at:
www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

1.40 The Radioactive Substances Act 1993

The Act applies to organisations that keep, use or dispose of radioactive material or waste. It is supplemented by the High-activity Sealed Radioactive Sources and Orphan Sources (HASS) Regulations 2005, which apply additional requirements on organisations that use or dispose of sealed radioactive sources, for example those used for radiography and radiotherapy. Organisations that keep or use radioactive material or sources must obtain a certificate of registration from the Environment Agency, while those that dispose of radioactive waste or sources must obtain a certificate of authorisation.

Information governance considerations

Records relating to radioactive substances and radioactive waste must be retained as specified by the Environment Agency. The Agency may also require that records be retained for a specified period after the activity has ceased. Once this period has expired, records should be filed with an appropriate repository, ie a Place of Deposit.

1.41 The Regulation of Investigatory Powers Act 2000

The Act regulates the power of government security services and law enforcement authorities by allowing the interception, surveillance and investigation of electronic data in specified situations such as when preventing and detecting crime. Powers include being able to require the disclosure of data encryption keys.

The main measures under the Act are as follows:

- It updates the law on the interception of communications to take account of technological change such as the growth of the internet.
- It also puts other intrusive investigative techniques on a statutory footing for the first time.
- It provides new powers to help combat the threat posed by rising criminal use of strong encryption.
- It ensures that there is independent judicial oversight of the powers in the Act.

The Act replaces the Interception of Communications Act 1985.

In addition, the Act empowers the Secretary of State for Health to make regulations that allow organisations to intercept communications in the course of lawful business practice and in specific circumstances without the express consent of either the sender or the recipient. Under the Regulations, organisations are required to make all reasonable efforts to inform the users of their systems that such interceptions might take place. These Regulations are the Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations.

The Regulations allow organisations to intercept communications without consent in the following circumstances to:

- establish the existence of facts (eg to obtain evidence of a business transaction);
- ascertain compliance with regulatory or self-regulatory practices or procedures relevant to the organisation (to ascertain whether the organisation is abiding by its own policies);

- ascertain or demonstrate standards that are achieved or ought to be achieved by persons using the system (eg staff training or quality control, but not for market research);
- prevent or detect crime (including crimes such as fraud as well as infringement of other IT-related legislation such as the Computer Misuse Act 1990 or the DPA 1998);
- investigate or detect unauthorised use of the systems (eg to check whether the user is breaking the Regulations);
- ensure the effective operation of the system (eg to protect against viruses or other threats such as hacking or denial of service attacks, to monitor traffic levels, or to forward emails to correct destinations);
- check whether or not communications are relevant to the organisation (eg checking email accounts when staff are absent on holiday or sick leave); and
- monitor (but not record) calls to confidential, counselling helplines run free of charge by the organisation, provided that users are able to remain anonymous if they so choose.

Information governance considerations

Staff with responsibility for information security management should be fully aware of the Act and its related Regulations, as these potentially impact information services used by the organisation's staff and others. Where interception or monitoring of communications or systems usage is locally permitted under the Act's provisions, it is essential that potentially affected individuals, the organisation's legal advisers and human resources department are all aware of this possibility. In such circumstances, it is advisable to notify staff in induction training and routine awareness programmes and at the point of system log-on of this possibility.

1.42 The Re-use of Public Sector Information Regulations 2005

These Regulations link with the FOI Act 2000, in that FOI is about access to information and these Regulations are about how the information can be re-used. However, there is no automatic right to re-use merely because an access request has been granted. Information that is exempt under the FOI Act or other legislation is also exempt under these Regulations.

Health service bodies are required to:

- publish the terms and conditions of standard licences for re-use;

- compile an information asset register detailing the information available for re-use;
- publish details of any exclusive re-use licences granted and review those licences every three years;
- notify the applicant of the reasons for refusal of a re-use application;
- provide contact details where complaints can be addressed;
- deal with all applicants in a non-discriminatory manner, for example applying the same charges for the same type of use; and
- respond to requests within 20 working days.

Information governance considerations

Employees responsible for re-use issues should work closely with those responsible for FOI for several reasons, including:

- an information audit is required for both pieces of legislation to determine the records held and the locations of those records;
- information available for re-use and the terms and conditions of re-use can be included within the organisation's publication scheme (see FOI Act 2000 on page 29); and
- if a request is made for access and re-use, the processes need to be co-ordinated so that the access issue is dealt with before permission to re-use is granted.

The Office of Public Sector Information provides further advice on the link between the FOI Act 2000 and these Regulations, and wording on re-use that can be included when responding to an FOI request, available at: www.opsi.gov.uk/advice/psi-regulations/advice-and-guidance/psi-guidance-notes/links-between-access-and-reuse.htm

1.43 The Road Traffic Acts

These Acts make provision for the establishment of a scheme to recover the costs of providing treatment to an injured person. The scheme is managed by the Compensation Recovery Unit (CRU), which is part of the Department for Work and Pensions.

Information governance considerations

NHS bodies are required by law to provide information to the CRU to enable the recovery of the costs of the treatment. The Road Traffic Acts require that NHS organisations give any information, which is in their power to give and which may lead to identification of a driver who has committed an offence under the Acts.

1.44 The Sexual Offences (Amendment) Act 1976, sub-section 4(1), as amended by the Criminal Justice Act 1988

This prohibits any information that would identify any rape victim from being included within a written publication available to the public or from being broadcast or included in a cable programme. The prohibition exists for the lifetime of the victim.

Information governance considerations

To meet the requirements of this legislation, organisations must ensure that they have processes in place to answer press enquiries about high-profile cases. If an interview is given to the press, particularly a live interview, it is vital that information is not inadvertently disclosed that could identify the victim.

Section 2 Relevant Standards and Guidelines

2.1 BSI BIP 0008

The title of this British Standard document is 'Legal Admissibility and Evidential Weight of Information Stored Electronically'. It sets a benchmark for procedures that should be followed in order to achieve best practice for the legal admissibility of electronic documents.

2.2 BSI PD 5000:1999

Entitled 'Electronic Documents and e-Commerce Transactions as Legally Admissible Evidence', the BSI Code of Practice PD 5000:1999 enables organisations to demonstrate the authenticity of their electronic documents and e-commerce transactions, so they can be used as legally admissible evidence.

The Standard contains five parts as follows:

- Information Stored Electronically (DISC PD 0008:1999);
- Electronic Communication and Email Policy;
- Identity, Signature and Copyright;
- Using Certification Authorities; and
- Using Trusted Third Party Archives.

2.3 British Standard 5454:2000

'Recommendations for the Storage of Archival Documents, including Library Materials'.

2.4 BS ISO/IEC 17799:2005; BS ISO/IEC 27001:2005; BS 7799-2:2005

This Standard provides a code of practice and a set of requirements for the management of information security.

The Standard is published in two parts. Part 1 has been adopted as ISO 17799:2005 and provides a code of practice for information security management. Part 2 provides a specification for information security management systems.

2.5 The Good Practice Guidelines for GP Electronic Patient Records v3.1

The General Practitioner's Committee, Royal College of General Practitioners and Department of Health defined guidance and interpretation of rules and standards for the adoption and use of electronic records within general practice.

2.6 BS ISO 15489-1:2001; PD ISO/TR 15489-2:2001

This is the international records management standard, it is published in two parts.

Part 1 provides best practice guidance on the management of records, in all formats or media, with advice on responsibilities and on the design and implementation of a records system. Part 2 is an implementation guide to Part 1.

2.7 ISO 19005-1:2005 – Document Management

The standard specifies how to use the portable document format (PDF) 1.4 for long-term preservation of electronic documents.

2.8 IT Infrastructure Library: ITIL Best Practice for Security Management

The publication is one in a series of ITIL guides produced by the Office for Government Commerce (OGC) dealing with IT infrastructure service management. It explains how to organise and maintain the management of security of the IT infrastructure from an IT manager's point of view.

2.9 Information Security Forum: Standard of Good Practice for Information Security

The publication is available from the website www.securityforum.org and contains the Information Security Forum's (ISF's) view of information security management best practices that are broadly equivalent to the BS 7799-2:2005. Other ISF publications will be considered for their relevance to future NHS information security management guidance and methods.

2.10 The NHS Information Governance Toolkit

The Information Governance Toolkit return is required from any organisation, including NHS and social care organisations, requesting an N3 connection or access to NHS Connecting for Health's digital information services and provides guidance and best practice on all facets of information governance including:

- information governance management;
- confidentiality and data protection assurance;
- information security assurance;
- clinical information assurance;
- secondary use assurance; and
- corporate information assurance.

For more information visit:
www.igt.connectingforhealth.nhs.uk

2.11 Records Management: NHS Code of Practice

The Records Management Code of Practice is the result of a Department of Health public consultation which included all NHS organisations and professional bodies.

The Code offers detailed guidance on:

- the management of all NHS record types;
- the day-to-day use of NHS records; and
- minimum retention period schedules for NHS records.

The Code can be accessed at:
www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

2.12 Information Security Management: NHS Code of Practice

The Information Security Code of Practice was published by the Department of Health as a guide to the methods and required standards of practice in the management of information security.

The Code can be accessed at:
www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_074142

2.13 Equality and Human Rights in the NHS: A Guide for NHS Boards

This Department of Health guide helps NHS Board members to understand and comply with their obligations under equality and human rights legislation.

The guide can be accessed at:
www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_062906

2.14 Governance Arrangements (for NHS Research Ethics Committees)

A standards framework for the process of review of the ethics of all proposals for research.

The framework can be accessed at:
www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4005727

Section 3 Professional Codes of Conduct

All the NHS professions have their own codes of conduct setting out the standards of ethical behaviour owed by members of each profession. These standards typically include:

- respecting patients' decisions about their care and treatment;
- obtaining consent for treatment or for disclosure of patient personal information;
- protecting patient personal information by maintaining confidentiality; and
- ensuring continuity of care through good record-keeping practice.

Information on professional codes of conduct can be obtained from the following organisations.

3.1 General Medical Council

www.gmc-uk.org/guidance/index.asp

3.2 Nursing and Midwifery Council: Code of Professional Conduct

www.nmc-uk.org/(sknklt551haimf55pdsrmd25)/aFrameDisplay.aspx?DocumentID=475

3.3 Nursing and Midwifery Council: Records and Record-keeping

www.nmc-uk.org/(k452wr55m2qj1p2ppgy3xf45)/aDisplayDocument.aspx?DocumentID=1120

3.4 Nursing and Midwifery Council: Midwives' Rules and Standards

The document provides the rules and standards for midwifery and the statutory supervision of midwives. It includes guidance on record keeping.

www.nmc-uk.org/(k452wr55m2qj1p2ppgy3xf45)/aDisplayDocument.aspx?DocumentID=169

3.5 Chartered Society of Physiotherapy: Rules of Professional Conduct

www.csp.org.uk/director/effectivepractice/rulesofconduct/professionalconduct.cfm

3.6 General Social Care Council: Codes of Practice for Social Care Workers and Employers

www.gscc.org.uk/Good+practice+and+conduct/What+are+the+codes+of+practice

3.7 Health Professions Council – Standards of Conduct, Performance and Ethics

www.hpc-uk.org/aboutregistration/standards/standardsofconductperformanceandethics/index.asp

3.8 Information on ethical practice

The British Medical Association produces a range of materials on ethical practice – see:
www.bma.org.uk/ap.nsf/Content/Hubethics

283473 1p 1.5k Sept 07 (FMP)
Produced by COI for the Department of Health

If you require further copies of this title quote
283473/NHS Information Governance and contact:

DH Publications Orderline
PO Box 777, London SE1 6XH
Email: dh@prolog.uk.com

Tel: 08701 555 455
Fax: 01623 724 524

Textphone: 08700 102 870 (8am to 6pm, Monday to Friday)

283473/Information Governance can also be made available on request in braille, audio, on disk and in large print.

www.dh.gov.uk/publications