

Confidentiality Policy

The Duty of confidence

1. NHS organizations and those carrying out functions on behalf of the NHS have a duty of confidence to patients and a duty to support professional ethical standards of confidentiality.
2. Everyone working for or with the NHS records, handles, stores or otherwise comes across information that is capable of identifying individual patients. All have a personal duty of confidence to patients and to his/her employer.
3. The duty of confidence is conferred by common law, statute, contract of employment, and professional registration.
4. This Policy is primarily but not exclusively concerned with patient confidentiality. The principles apply equally to information regarding other individuals, including staff.

What is confidential information?

5. Confidential information is information entrusted by an individual in confidence, where there is a general obligation not to disclose that information without consent.
6. Confidential information may include personal information such as name¹, age, address, and personal circumstances, as well as sensitive information regarding race, health, sexuality, etc.
7. Confidential information may be known, or stored on any medium. Photographs, videos, etc are subject to the same requirements as information stored in health records, on a computer, or given verbally.
8. Person-identifying information (i.e. that which identifies individuals personally) is assumed to be confidential, and should not be used unless absolutely necessary. Whenever possible, anonymised data—from which personal details have been removed and which therefore cannot identify the individual—should be used instead. Note however that even anonymised information can only be used for justified purposes.

Awareness and compliance

9. Everyone in the Trust must be aware of the importance of confidentiality, and their responsibilities for safeguarding confidentiality and keeping information secure.
10. Staff must comply with the requirements of the Caldicott Report, the Data Protection Act 1998 (see Appendix 1), The NHS Confidentiality Code of Practice, and the Trust's Information Protection Policy and Guidelines.
11. Breaches of confidentiality are a serious matter. Non-compliance with this policy may result in disciplinary action being taken. No employee shall knowingly misuse any information or allow others to do so.

¹ However, it is not necessarily a breach of confidentiality to call out the name of a patient in a waiting room, or for a ward or other clinical unit to maintain a list of patients and their location for identification purposes.

Acting on the duty of confidentiality

12. No personal information, given or received in confidence, may be passed to anyone else without the knowledge and consent of the provider of the information. This is usually the patient but sometimes another person (e.g. relative or carer) may be the source.
13. No personal information, given or received in confidence for one purpose, may be used for a different purpose without the consent of the provider of the information.
14. Patients have the right to object to the use of their personal health data for purposes other than their immediate care.
15. The duty of confidentiality owed to a deceased patient should be viewed as being consistent with the rights of living individuals.

Disclosing information

16. Information concerning individuals may be passed on to someone else only:
 - on a 'need to know' basis;
 - when the disclosure is necessary for the clinical care of a patient (e.g. between members of a clinical or multidisciplinary team);
 - when required for the safe and effective management of the Trust and its services;
 - there is a statutory or legal obligation to do so.
17. In most instances, information may only be disclosed with the patient's consent. The Trust has an obligation to ensure that its patients are fully informed regarding the uses to which it puts information gathered about them. Provided that patients have been so informed, staff may normally disclose information where this is in the best interests of the patient (e.g. for routine clinical care) but a patient with capacity may refuse such disclosure, and where there is reasonable doubt, the patient should be asked and refusal of consent must normally be respected.
18. Certain statutory and legally-required disclosures may not require consent, although the patient must always be informed when such a disclosure is made.

Responsibilities

19. The Caldicott Guardian is responsible for overseeing and advising on issues of confidentiality and information protection for the Trust.
20. Managers are responsible for ensuring that all staff, including temporary staff, contractors and volunteers, know what is expected of them with respect to confidentiality and protecting information.
21. All staff are responsible for adhering to this Policy and following the associated guidelines, and for safeguarding the confidentiality of all personal and Trust information, transmitted or recorded by any means.

Version Control

Susan Haimes/ Chris Bunch	Version 1.7	Approved by Trust Board November 2002
Chris Bunch	Version 2.0d	March 2008
Chris Bunch	Version 2.1	Trust Board May 2008

Confidentiality Guidelines

Introduction

1. Everyone working for or with the NHS who records, handles, stores or otherwise comes across information that is capable of identifying an individual patient, has a personal duty of confidence to that individual and to his/her employer.
2. These Guidelines aim to stress the main principles behind maintaining confidentiality. Further guidance may be obtained from the General Medical Council² and the Department of Health³, amongst others.
3. Whilst primarily though not exclusively concerned with patient confidentiality, the principles reflected in these guidelines apply equally to information regarding other individuals, including staff.

Disclosure of confidential information

4. When information is passed from one to another, it is said to have been *disclosed* to the recipient. Good practice in maintaining confidentiality is mainly about ensuring that patients are aware when and why disclosures occur, and that such disclosures are necessary, appropriate, and undertaken safely and securely.
5. In many situations it may not be strictly necessary to disclose the identity of the patient. For example, it is often sufficient to communicate or discuss just the clinical details in order to obtain advice about management of a particular patient.

Inappropriate disclosure

6. Inadvertent or inappropriate disclosure of confidential information is potentially a serious matter. Adherence to the following principles will reduce the risk of this occurring.
7. If you are uncertain whether information is confidential or not, assume that it is.
8. Whenever possible, remove person-identifying details (e.g. name and address) and use other information such as the NHS number.
9. Do not give out information unless you are certain that the requestor has a right to receive it. Be especially careful on the telephone: always check the identity of the caller and the individual about whom they are enquiring. Do not automatically assume that they have a right to the information.
10. Do not talk about confidential matters where you can be overheard, e.g., near another patient, in the queue at the canteen, in a lift, etc. Be careful not to leave or inadvertently display confidential notes in public places.
11. Never look up patient information systems such as PAS, CaseNotes or PACS unless you need to know because of your involvement in the care of the patient. For example, you

² General Medical Council. Confidentiality: Protecting and providing information.

³ Department of Health 2003. Confidentiality: NHS Code of Practice.

must not look up information on family, friends, celebrities or indeed anyone else out of either curiosity or because you have an interest in doing so outside any clear professional duty of care to that patient.

12. Always check fax numbers yourself with the intended recipient before you send information by fax. Use safe haven areas and call to say the information is being sent.
13. Make sure that case notes and other confidential papers cannot be overlooked or accessed by unauthorised personnel and that computer screens are not situated where they can be viewed by unauthorised personnel
14. Make sure that less obvious sources of person-identifying data, such as notebooks, diaries, appointment books, etc. are kept securely, and disposed of when they are no longer required.
15. Be particularly careful if work is taken home: the Trust is still responsible for the data and it must be kept secure at all times. Patient records may not be taken home without permission from the Medical Director or Caldicott Guardian.
16. E-mail systems are inherently insecure: do not send confidential information by e-mail unless absolutely necessary and only if encrypted. See the Trust's *Information Protection Policy and Guidelines* for further information.
17. Confidential papers must be securely packaged if they are to be transported or sent to another location. The Trust's *Information Protection Policy and Guidelines* has further information transferring confidential information by post.
18. Always dispose of confidential material by the proper means. Papers must be put in designated confidential waste bags or bins, and send for shredding. To dispose of information stored on computer disks, call the ICT Contact Centre on 22822 and request that they be removed by an analyst for disposal.

Relatives and friends

19. In most circumstances, patients will usually want close relatives to be informed about their diagnosis and care, but this may not always be the case and relatives and friends *do not have the right to any information* about a patient without that patient's consent.
20. In the case of patients with capacity it is important that staff discuss with the patient who may be informed, if anyone. In the case of patients who lack capacity to consent to this, staff have a general obligation to act in the patient's best interests and this will normally mean that staff will need to discuss confidential matters with one or more close relatives or friends. The substance of such discussions should be documented in the patient's records, and regularly reviewed and updated.
21. In the case of minors (i.e. those aged under 18 years) who lack capacity to consent to disclosure, staff should normally inform parents (strictly those with parental responsibility) of all information relevant to the care and management of the patient. Staff will need such parental consent in order to care for the patient. Patients aged 16 and 17 years who have capacity normally have the right to determine who should know confidential information about them. In the case of those aged less than 16 years, the person is

presumed to lack capacity but if s/he has capacity then s/he may give or withhold consent to inform relatives and friends.

Disclosure in the public interest⁴

22. Disclosure of personal information without consent may be justified where failure to do so may expose the patient or others to risk of death or serious harm. Where third parties are exposed to a risk so serious that it outweighs the patient's privacy interest, you should seek consent to disclosure where practicable. If it is not practicable, you should disclose information promptly to an appropriate person or authority. You should generally inform the patient before disclosing the information.
23. Such circumstances may arise, for example:
- Where a colleague, who is also a patient, is placing patients at risk as a result of illness or other medical condition. If you are in doubt about whether disclosure is justified you should consult an experienced colleague, or seek advice from a professional organization. The safety of patients must come first at all times.
 - Where a patient continues to drive, against medical advice, when unfit to do so. In such circumstances you should disclose relevant information to the medical adviser of the Driver and Vehicle Licensing Agency (DVLA) without delay.
 - Where a disclosure may assist in the prevention or detection of a serious crime. Serious crimes, in this context, will put someone at risk of death or serious harm, and will usually be crimes against the person, such as abuse of children.
24. Such disclosures must be made in good faith, in the belief that the information is true, and where the disclosure is not made for personal gain

Disclosure to the Police

25. There is no absolute requirement to disclose, or not to disclose information to the police. NHS guidance is that information should be disclosed to assist the police with the prevention or detection of serious arrestable offences.
26. Although there is no absolute definition of serious crime, the criminal evidence Act 1984 lists serious arrestable offences as:
- treason, murder, manslaughter, rape, kidnapping, certain sexual offences, causing an explosion, certain firearms offences, hijacking, causing death by reckless driving, offences under prevention of terrorism legislation;
 - where a court order is presented requiring the information;
 - where a threat is made, which if carried out would be likely to lead to death or serious injury, substantial financial gain or loss, serious interference with the administration of justice or investigation of an offence.
27. Theft, fraud and burglary (unless aggravated by assault) are unlikely to outweigh the duty of confidentiality to the patient. Information should not be disclosed in these cases. Seek guidance from the legal services department if in doubt.

⁴ Adapted from General Medical Council: *Confidentiality: Protecting and providing information*.

Other disclosures

For other situations, such as disclosures to the Press and media, Solicitors, and disclosures required under Statute (i.e. by law) please see Appendix 3.

Consent for the use of information

28. Consent for the use of personal information is not the same as consent for carrying out clinical procedures, although it is often associated with a healthcare episode.
29. Implied consent for the use of identifiable information is no longer necessarily sufficient. It is acknowledged that it is not possible for explicit consent to be obtained for the use of data in all circumstances, although this is preferred.
30. Instead, patients are expected to give *informed* consent. Informed consent means that the patient makes a decision having been given sufficient information explaining the uses to which information (about them) may be put, and their rights with respect to the use personal information about them. The Trust requires that all patients are given a copy of the leaflet Information for Patients, which contains a section on the use of information, and that posters covering the same information be displayed prominently in all patient reception areas.
31. In normal circumstances, patients have the right to object to the use of their personal health data for purposes other than their immediate care. If consent is withheld, the possible consequences for the care of the individual must be clearly explained, but their decision must be respected unless circumstances are exceptional, for example as described about under Disclosures in the public interest, and Disclosures to the Police.
32. The reasons for any refusal of consent must be documented in the patient's notes.
33. Where a patient is not competent to consent, decisions regarding the use of that information must be made in the patient's best interests by those responsible for providing care, if necessary seeking the advice of the relevant senior clinician.

Subject access

34. People are entitled, under the Data Protection Act 1998, to see information about themselves and to have copies of it if they wish (a Subject Access Request). There are some restrictions to the release of information⁵.
35. All Subject Access queries should be directed to the Health Records Manager. There may be a charge for this service.
36. By law, people must be given an explanation of any terms or abbreviations that are not easy for a layman to understand.
37. Staff should ensure that all relevant facts and discussions are recorded, however the information should always be defensible. Including colloquial expressions of opinion about patients is most unwise.

⁵ Guidance on the restrictions can be obtained from the Health Records Dept. or Information Security Office

Incidents and breaches of confidentiality

38. If you think that confidential information may have been revealed by accident, or by other means (for example theft of papers or a computer), it is essential that you complete an incident form and report it.
39. This enables monitoring of information incidents as a whole, and investigation of individual incidents where necessary. It is an important part of ensuring that practice improvements are brought in where necessary, and improving the service for patients.

Further information

40. Department of Health. The NHS Confidentiality Code of Practice.
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253
41. General Medical Council. Confidentiality: Protecting and Providing Information.
<http://www.gmc-uk.org/guidance/current/library/confidentiality.asp>
42. Oxford Radcliffe Hospitals Information Protection Policy and Guidelines

Appendix 1: Caldicott, legal and professional requirements

Caldicott principles

1. The Caldicott Report was commissioned by the Chief Medical Officer in 1997, in response to growing concerns about the risk to patient confidentiality with the increasing use of computers in healthcare.
2. The report contains 16 recommendations, and 6 good practice principles. NHS organisations have to report annually on their progress towards Caldicott compliance against 18 headings (which do not correlate directly with the recommendations or the principles).
3. Each NHS Trust is obliged to appoint a senior clinical member of staff to act as Caldicott Guardian for the Trust, to oversee issues of confidentiality. The Caldicott Guardian for the Oxford Radcliffe Hospitals is Dr Chris Bunch.
4. The six Caldicott principles are:
 - Principle 1 Justify the purpose for each use/transfer of patient-identifiable information.
 - Principle 2 Don't use patient-identifiable information unless it is absolutely necessary.
 - Principle 3 Use the minimum necessary patient-identifiable information.
 - Principle 4 Access to patient-identifiable information should be on a strict need-to-know basis.
 - Principle 5 Everyone with access to patient-identifiable information should be aware of their responsibilities.
 - Principle 6 Understand and comply with the law.

The Data Protection Act 1998

5. The Data Protection Act 1998 came into force in March 2000. Its purpose is to protect the right of the individual to privacy with respect to the processing of personal data. The Act laid down eight data protection principles:
 1. Data must be processed fairly and lawfully.
 2. Personal data shall be obtained only for one or more specific and lawful purposes.
 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
 4. Personal data shall be accurate and where necessary kept up to date.
 5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
 6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection 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 outside the European Union, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Human Rights Act

6. As an employee of a public authority you have a duty to comply with Article 8 of the Human Rights Act 1998. This states that everyone has the right to respect for his/her private and family life, home and correspondence. There should be no interference with this right unless necessary in the interests of protecting public health and safety or preventing crime

1990 Computer Misuse Act

7. The 1990 Computer Misuse Act makes it a criminal offence to gain or attempt to gain unauthorised access to any program or data held in any computer. The more serious offences under the Act are:
 - gaining, facilitating or attempting to gain unauthorised access to any program or data held in any computer, with the intent to commit further offences under the Act;
 - carrying out any unauthorised action which is intended to modify the contents of any computer.
8. Anyone who tries to access a computer or system, or information thereon, to which they do not have authorised access rights is committing an offence. Modifying or attempting to modify information or programs is also an offence, and this would include introducing a virus into a computer or system.

Appendix 2: Third Party enquiries and disclosures

1. **Press and Media:** No member of staff should attempt to answer questions from any media organisation or individual, but should refer all Press and Media enquiries to the Communications Team
2. **Solicitors and Legal Representatives:** Solicitors acting on behalf of patients have some rights of access to information for their clients. Do not disclose any information yourself, but refer them to the Legal Services Department.
Legal Services Department 01865 222572
Oxford Radcliffe Hospitals NHS Trust
The Stable Block,
The John Radcliffe Hospital
Headley Way
Headington
Oxford OX3 9DU
3. **Complaints about Treatment or Care:** Formal complaints from patients, relatives or others should be directed to:
The Complaints Manager 01865 228966
Oxford Radcliffe Hospitals NHS Trust
The John Radcliffe Hospital
Headley Way
Headington
Oxford OX3 9DU
4. **Enquiries about the Trust and Trust procedures:**
The Corporate Services Manager, 01865 221383
Oxford Radcliffe Hospitals NHS Trust
Level 3, Academic Street,
The John Radcliffe Hospital
Headley Way
Headington
Oxford OX3 9DU

Mandatory disclosures and disclosures under statute

Circumstance:	Disclosure By:	Disclosure To:
Notifiable infectious diseases	Doctor currently responsible for patient's care and welfare	The Chief Environmental Health Officer of the relevant local authority, through the consultant in communicable Disease Control on Environmental Health and Protection Notification Certificates
Poisonings and serious accidents at the workplace	Doctor currently responsible for patient's welfare	To the Health and safety Executive via the Personnel Department of on-call manager using form UCH291. The information should be reported as soon as possible and does not have to wait till the next working day.
Abortions	The doctor who terminates the pregnancy	To CMO (DSS) on form HSA4
Drug addicts	The doctor in attendance	CMO (Home Office) on form FO9 – Notification of Drug Addiction
Births	Member of staff attending the birth	Child Health Department on Form SP7198 CH1 – Notification of Births
Road Traffic Accidents		There is no duty of disclosure except in order to obtain payment for treatment, The police must obtain the doctor's consent before obtaining to obtain a specimen from the suspected patient. See also 'Disclosure to the Police': information may be requested if an offence of death by dangerous driving may have been committed

Bodies empowered to order disclosure

- A Court of Law (including Coroners Court and Industrial Tribunals)
- Health Service Commissioner
- Health and Safety Commission
- Health and Safety Executive
- Inquiries appointed by the Secretary of State
- Employment Medical Advisers
- Professional bodies of the Health Professions – doctors, dentists, nurses, midwives, health visitors, opticians and professions allied to medicine (but not pharmacists)
- Mental Health Act Commission
- Mental Health review Tribunals

5. Disclosures to non-NHS organisations such as social services may be essential to the continuing care of the individual but must be strictly controlled.
6. **Additional categories:** No information should be disclosed to the following agencies unless in exceptional circumstances, or with the consent of the patient.
 - Department of Social Security (DSS / Benefits Agency). The patient's consent must be obtained before notifying the Benefits Agency of their stay in hospital.
 - Employers
 - Schools
 - Police (unless in conjunction with prevention or detection of serious crime: treason, murder, manslaughter, rape, kidnapping, certain sexual offences, causing an explosion, certain firearms offences, hijacking, causing death by reckless driving, offences under prevention of terrorism legislation).

Appendix 3: Information for patients on the use of their information

1. The following is available as an information leaflet for patients.

Your information and how we use it

Your personal health information

1. Every time you come into hospital, information about you, your medical treatment and family background may be recorded, on paper and computer, to help us provide you with healthcare services. The information forms part of your Health Record and will be kept in case we need to see you again.
2. Members of the NHS team looking after you may share your personal health information with each other. This team may include nurses, doctors, therapists, pharmacists, laboratory staff and clerical support staff plus students and trainees in medicine or other healthcare professionals who are looking after you.
3. Please note ALL staff working and training in the NHS are bound by law and a strict code of confidentiality and are regulated and monitored by the Trust's Caldicott Guardian (an NHS appointed role responsible for ensuring patients' rights to confidentiality are respected).

How your records are used to help you

4. The staff involved in your treatment need to have accurate and up-to-date information to assess your health and provide you with care.
5. A record of any treatment or care you receive in hospital will be kept in case you return for further treatment and to assist other NHS staff who treat you in the future both in the hospital and elsewhere.
6. Your records allow hospital staff to assess and investigate the type and quality of care you have received should the need arise.

How your information can help the NHS

- to enable us to review the care provided for you and other patients, to ensure it is of the highest quality, make sure our services can meet all patients' needs in future and enable the production of NHS-wide statistics;
 - to train healthcare professionals and support hospital research and development;
 - to enable the hospital to be paid for your treatment and to support audits of NHS services and accounts;
 - to support the investigation of any incidents or issues that arise.
7. In addition, information may be used for Research Projects that have been approved by the Local Research Ethics Committee. You will be asked for your consent if we need to use any information that clearly identifies you. For instance, some research studies identify people so that information from the research can contribute to their future care.

Sharing your information

8. Sometimes the Trust is required to pass on information by law, for example:

- to notify a birth;
 - when an infectious disease is encountered that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS);
 - where a formal court order has been issued.
9. You may receive care from non-NHS staff (for example Social Services), with whom it is necessary to share information about you to enable them to work with medical staff in providing your care. Your information will only be made available if there is a genuine need for it and where your consent is needed we will contact you for permission.
10. The principal NHS partner organisations with which information may be shared are Strategic Health Authorities, other NHS Trusts, GP practices and the Ambulance services. If it is necessary to pass on information about you, personal details are removed whenever possible.

Your information rights

11. You have the right to know how we will use your personal information. This poster aims to provide you with this information.
12. You have the right of access to your Health Record (your medical notes). This is known as *Right of Subject Access*.
13. You have the right to object to us making use of your information.
14. You can ask us to change or restrict the way we use your information and we are obliged to agree if it is possible to do so.
15. You have the right to ask for your information to be changed, blocked or erased if the information we are holding about you is incorrect.

To make a Subject Access Request

16. If you are staying in the hospital, you may ask to look at your Health Record folder. Your notes will be prepared for your viewing and a qualified member of staff will talk you through its content.
17. You should be aware that in certain circumstances your right to see some details in your health records may be limited - for example if it would reveal third-party information.
18. If you would like to see your Health Record after you leave hospital, or if you would like copies of your Health Record, you will need to send a written request, called a Subject Access Request, to the Health Records Manager for the Trust. For further information please visit:
<http://www.oxfordradcliffe.nhs.uk/forpatients/healthrecord.aspx>
or call 01865 221516/ 221621/ 221856

Information protection policy

Introduction

1. Legislation, Department of Health Guidelines and NHS Policies require NHS organisations to have written policies and procedures covering the collection, storage, processing and disclosure of personal and confidential information in both manual and electronic systems.
2. This policy document, and the accompanying document entitled 'Information Protection: User Guidelines' set out these procedures for the Oxford Radcliffe Hospitals NHS Trust.
3. The Data Protection Act 1998 regulates the processing of information relating to living individuals, including collection, storage, use, and disclosure. The Act came into force on 1st March 2000.

Policy

4. The Trust will seek to prevent improper or unlawful disclosure of information collected, processed and stored by the Trust (including patient, business, administrative, research, professional and staff information).
5. The Trust will promote the central principles of confidentiality, integrity and availability that are at the core of the NHS Information Governance requirements.
6. The Trust will implement the requirements of appropriate current legislation and available guidance to ensure the successful achievement of these aims.

Responsibilities

7. A senior clinician is appointed as the *Caldicott Guardian* for the Trust.¹ The Caldicott Guardian has direct access to the Trust and Executive Boards and is *inter alia* responsible for:
 - establishing standards for information protection, and
 - overseeing issues of patient confidentiality within the Trust.
8. The Director of Planning and Information acts as the Data Controller within the meaning of the Data Protection Act 1998, and has overall responsibility for:
 - maintaining the Trust's registration under the Data Protection Act 1998;
 - the development and maintenance of the procedures set out in the information protection guidelines;
 - ensuring that any outsourced information management and technology functions are supported by appropriate Service Level Agreements, and that these reflect the requirements of this policy;
 - ensuring that any external organization processing or handling data or information on behalf of the Trust have in place equivalent information protection policies and procedures that are approved by the Trust;

¹ The establishment of Caldicott Guardians is a recommendation of the report of the Caldicott Committee on the Review of Patient-Identifiable Information, issued in by the Department of Health in December 1997. The Caldicott Guardian at present is Dr Christopher Bunch.

- providing advice on the secure management of information;
 - providing advice to staff on the risks of poor information management;
 - monitoring breaches of the information protection policy and procedures;
 - raising incident reports through the Trust's incident reporting mechanism;
 - maintaining this Policy.
9. The responsibilities of the Caldicott Guardian and the Data Controller will be maintained on a day-to-day basis by the Information Governance and Records Manager.
10. Responsibility for the maintenance and security of the Trust's data network and computer hardware rests at present with the *Oxfordshire Health Information Services (OHIS)*. Trust personnel must at all times abide by such regulations and standards required by OHIS for the proper discharge of their duties.
11. Departmental and directorate managers and information governance leads are responsible for:
- ensuring that the procedures described in the accompanying user guidelines are implemented;
 - making available to their staff copies of the current Information Protection Policy and User Guidelines;
 - ensuring that all staff have a copy of the staff summary, contained at the back of the accompanying user guidelines;
 - ensuring that staff have the necessary skills and training to enable them to follow the procedures.

Individual staff members are responsible for:

- protecting the integrity, availability and confidentiality of trust information;
- acting to prevent the improper use or disclosure of information;
- following procedures as set out in the accompanying user guidelines;
- reporting breaches of the Trust Information Protection Policy through the Trust incident reporting procedure;
- ensuring the safe collection, storage, processing and disclosure of personal and confidential information in any medium;
- attending relevant training sessions as required.

Authors

Susan Haimes, David Dickens & David Hopkins (2000)
Revised 2008 by Chris Bunch and Kathy Hulcup

Version control

Version 3.1 Approved by Trust Board 14th April 2000
Version 4.0d Draft March 2008
Version 4.0 To Trust Board May 2008.

Revision due

April 2011.

Information protection guidelines

Introduction

1. NHS organisations are required to have written policies and procedures covering the collection, storage, processing and disclosure of personal and confidential information in organised manual and electronic systems. Some elements of the guidance relate to laws, others concern good practice, sensible management and effective organisation.
2. The Data Protection Act 1998 regulates the processing of information relating to living¹ individuals, including obtaining, using, storing and disclosing it. The Act comes in to force on 1st March 2000.
3. The secure management of data has become a greater challenge in recent years, partly as a result of improving capabilities in information technology and the consequent increase in the mobility of stored information.
4. These guidelines and the accompanying Information Protection Policy set out how the Trust aims to comply with the requirements of legislation and NHS guidance.
5. All staff have an obligation to safeguard the information they encounter at work, in whatever format. This is governed by law, employment contracts, and by professional codes of conduct.
6. If members of staff have any questions about the issues raised in the document, or related matters, they are encouraged to speak to their manager or to the Information Communications and Technology (ICT) Helpdesk on Extension 22822.
7. The aims of this document are:
 - to set out procedures for the management and protection of information generated, stored, processed or disclosed by the Trust;
 - to ensure that staff are aware of the relevant legislation and guidance;
 - to minimise the risks faced by patients and staff in using and managing information; and
 - to provide a grounding in information protection issues for Trust staff.
8. To achieve these aims:
 - the procedures in this document must be followed;
 - all new manual and electronic systems, or new uses of existing systems, must be notified to the ICT Department so that they can be used to update the Trust's registration under the Data Protection Act 1998;
 - a copy of this document should be distributed to relevant staff. The document will be available for download from the Trust's Intranet;
 - A copy of the staff summary (at the end of the booklet) should be given to all staff;
 - all computers, systems and software that are used within the Trust should be registered with the Trust ICT inventory, held by the ICT Department.

¹ Data relating to deceased individuals is covered by the Access to Health Records Act 1990.

9. These guidelines have been written to promote the central principles of confidentiality, integrity and availability:

Confidentiality:	Information access is confined to those with the authority to view the information.
Integrity:	System assets are operating correctly according to specification and in the way the current user understands them to be operating.
Availability:	Information is delivered to the right person, when it is needed.

Information

10. In this document, information is defined as any kind of knowledge, data or facts that are recorded, transmitted or known.
11. All types of information held by the Trust—whether written, verbal, aural, visual (images), manual (paper-based) or electronic—and all categories of information used by the Trust—e.g. personal, patient, audit, employee, financial, risk management, legal—are covered by the Trust Information Protection Policy and by these guidelines.
12. Some information is *confidential*, and needs to be kept securely at all times. This includes all information concerning identifiable individuals, although many other items of information may be classified as confidential, for example business and financial data. In many instances confidential and non-confidential information are stored side-by-side and it is safer therefore to apply strict standards of security to all forms of information.
13. The term *person-identifying information* is used in this document to mean any information or data from which the identity of the individual to whom the information relates may be discerned. The handling of such information is governed by the Data Protection Act 1998 and the Caldicott confidentiality principles (see Appendix).

Confidentiality

14. NHS organizations and those carrying out functions on behalf of the NHS have a duty of confidence to patients and a duty to support professional ethical standards of confidentiality.
15. Confidentiality means that individuals are trusted not to disclose certain items of information. Security is keeping things safe from unauthorised access.
16. Confidential information includes not only patient records, but conversations, forms, employee information, computer files and so on. It applies to personal non-health information such as name, address and details of financial or domestic circumstances as well as to clinical data.
17. GMC guidance to doctors states that “*Without assurances about confidentiality patients may be reluctant to give doctors the information they need in order to provide good care*”.
18. The Caldicott principles governing confidentiality are listed in Appendix x. The Trust’s *Confidentiality Policy and Guidelines* cover the requirements in more detail.

Protecting information

Physical protection and security

19. Most computer equipment can be moved, and is therefore vulnerable to theft and damage. Aside from the loss of the equipment, this means that information may be lost, damaged or compromised. Manually stored information is also at risk.
20. Access to unsecured equipment or documents may also lead to data being altered, destroyed or copied.
21. The following measures will help to reduce the risk of accidental damage or theft of equipment and information:
 - ensure that all hardware that stores information is permanently marked as Trust property by the Trust Security Office;
 - ensure that any equipment in a vulnerable position, e.g. in public access areas, is secured to an object which cannot be easily moved;
 - ensure that disks and other removable information storage media, including paper documentation, are stored securely;
 - close all windows outside office hours, and draw the blinds. Lock or bolt the windows if possible;
 - lock doors when offices are not in use;
 - do not keep computers where they are at risk of accidental damage (i.e. near to water supplies, behind doors, on the floor etc);
 - ensure that portable computers are stored securely when not in use;
 - record serial numbers, versions and details of all hardware and software that you possess. Keep the details in a safe place and pass this information to the ICT department whenever additional equipment is obtained;
 - report any lost keys, ID badges or suspicious people to Trust Security immediately (Extension 444);
 - challenge people that you don't recognise;
 - ensure that sensitive information is not sent to printers or fax machines in areas with public access;
 - ensure that documents and computer screens are not viewable by people not entitled to see them.

Backing up/safe storage of information

22. Backing-up information regularly is essential to guard against accidental loss or damage. Backups of corporate systems, such as the Patient Administration System, (PAS) are taken centrally on a regular basis.
23. Backups form an important part of the Risk Assessment and Disaster Recovery Planning process.
24. Each information system (electronic or paper-based) must have a system manager, who is responsible for ensuring that the system is backed up. Backup procedures should be detailed

in a written document; in addition, critical systems should have a written disaster recovery plan, lodged with the ICT Department.

25. The user is responsible for backing up individual PCs that are not normally backed up centrally or locally. If the PC is used by more than one person, ensure that someone is given responsibility for backing up the computer.
26. When backups are made, consider the following:
 - it should be possible to recover the system completely from the backup should total failure occur. The recovery process should be enacted periodically to ensure that this can be done successfully;
 - backups should be kept securely, separate from the original information;
 - backups made for business continuity or other purposes must be made and kept in accordance with the Data Protection Act 1998.
27. If you would like more information about how to make backups, or if your computer or system needs a backup, contact the ICT Helpdesk (Ext. 22822).

Viruses

28. Computer 'viruses' are normally small programs that replicate themselves within or between computers, and can corrupt information on affected computers.
29. Viruses can be acquired from a number of sources, including software, e-mail file attachments, shared files obtained from or carried on removable media, the internal Trust computer network, the Internet, and other network connections.
30. Saving files that are to be attached to e-mails in portable document (.pdf) or rich text formats (.rtf) considerably reduces the risk of virus transmission.
31. Trust computers and systems are required to have virus-checking software installed, which should be up-graded regularly at intervals as advised by the ICT department². This software will detect the presence of virus code on the computer, notify the user, and enable its removal.
32. If you find a virus of any kind on your computer or system, contact the ICT Helpdesk (Extension 22822) as soon as possible.

Software

33. Software and programs used on any Trust system or computer must be acquired legally. In the case of licensed software, each copy must be licensed, and each individual computer or system must adhere to the relevant licensing agreement. These agreements vary from product to product.
34. The Trust has intellectual property interests in software produced within the Trust. Such software may not be distributed outside of the Trust without specific permission.

² For computers connected to the Trust's data network which have antivirus software installed, upgrading is done automatically.

35. Unlicensed software, shareware, and free software available through the Internet or supplied free with magazines may be incomplete or carry viruses, and must not be installed on Trust computers without authorization from the ICT Department.
36. Both the user and the Trust are liable for prosecution if software or programs are being used illegally. Care should be taken with licensed evaluation software to ensure that specific licensing conditions are not breached. For more information, please contact the ICT Helpdesk (Ext. 22822).

Passwords

37. Passwords are used to control access the Trust's network and to individual computers or systems. A generic network login and password is currently available for PCs/workstations used by multiple users in shared clinical areas, but this facility will shortly be replaced by single-user access using smart cards, as part of the wider NHS information systems programme. Passwords for access to specific information systems however must be specific to individual users.
38. Passwords are usually set at several levels.
 - *Individual PCs.* Where a PC is connected to the Trust's network (the vast majority), a password will be supplied by the ICT Department which will enable the user to login to Windows and the assigned network domain.
 - *Remote system access.* At present, each individual system (e.g. PAS, laboratory and radiology systems) create individual user accounts and passwords. Typical clinical users will therefore have different usernames and passwords for each system.
 - *Single login access.* To simplify this, the Trust is investigating a single login process which will provide users access to all the systems with which they are registered.
39. When accessing any system, you may only view information that you are entitled to. For example, on a patient or clinical system you may only access information about patients for whom you have responsibility. All accesses are logged, and it is an offence to view information about patients unless you have a legitimate reason to do so.
40. Access to applications sponsored by the national Programme for IT is governed by a specific registration process. All such applications will use a common approach to confidentiality and security, based on the individual user's role and responsibilities. Details are set out in the Trust's *Registration Authority Policy*.
41. There are important rules regarding passwords:
 - Your password(s) **must not** be disclosed to anyone else, nor should you use anybody else's password to gain access to a computer or system.
 - If others have gained knowledge of your password, or you are concerned that someone else may be using it, change it immediately and report the matter to the system manager.
 - Passwords must be changed regularly, at least every two months. For most corporate systems this is automatically enforced.
 - When constructing a password, ensure that it can't be guessed easily, and don't use words, phrases or number sequences (such as your name, user ID, date of birth, favourite football team, car number plate, telephone number, or anything that

relates to the user or the system). A good password will be at least eight characters long, and contain both letters and numbers.

- When leaving your computer unattended, make sure that you log out of any systems are logged in to, and that your computer either has a password-protected screen saver operating or is switched off.

Portable information storage media and portable computers

42. Portable information storage media means any kind of material or device that can be used to copy or store information, or to move information from one computer to another. Examples include any kind of disk, information storage tape, CD-ROM, CD-writable or CD-rewritable, removable hard drive, USB memory stick, palmtop or laptop. Risks associated with laptops and palmtops are greater, as they are capable of reading and displaying information as well copying, storing or moving it.
43. You are responsible for any information you transfer from a computer onto any portable device or media. Confidential information (including any person-identifying information) **must** be encrypted before transfer³, and remain encrypted on the device to which it is transferred. You should always consider carefully whether the data being transferred needs to include person-identifying items, and remove these if they are not strictly necessary.
44. When you encrypt data, you must also keep the key or access code safe and secure. If there is any doubt about the subsequent ability to gain access to the encrypted data in extreme emergencies, the ICT department can also store securely the key or access code.
45. The media must be kept safely, and the information removed or destroyed once it has served the purpose for which it was created. Using the 'delete' command is not sufficient to prevent the recovery of information, neither will re-formatting a disc completely remove the 'fingerprint' of information previously stored. Where sensitive information is concerned, the disk should be either destroyed, or overwritten with random data a number of times. Special software to enable you to overwrite with random data in this way can be obtained from the ICT Department.
46. You must have your manager's permission to take any personal or other sensitive information off the Trust's premises. In the case of medical facts, the Medical Director must be consulted.

Fax machines

47. All personal or other confidential information should be transmitted whenever possible using a fax located in a "safe haven" or area that can securely receive faxes without it being seen by unauthorised personnel.
48. Make sure that the individual who will receive the fax is entitled to see that information.
49. Before dialling, check yourself that the number to be dialled is the correct number. Do not rely on third hand details. When dialling, ensure that you are entering the number correctly, using the display if possible.

³ Until the NHS agrees an encryption standard, the Trust recommendation is to encrypt files using WinZip. Further advice may be obtained from the ICT department.

50. If the Information is confidential, then make sure that there is a person waiting at the receiving fax for your transmission, and ask them to call you back when the transmission is complete.
51. Obliterate any patient identifiers from the material to be faxed, label the resulting spaces, and supply the information verbally via the telephone once the fax has been received by the appropriate person.
52. Maintain fax call logs and keep them in a secure place.
53. If you send faxes to the wrong fax machine by mistake, or receive a fax that is not meant for you, a Trust incident report must be completed.

E-mail (internal and external)

54. E-mail (electronic mail) is widely used both inside and outside the Trust. It is extremely useful as a rapid and informal communication medium, but it is inherently insecure and there are special considerations where confidential information is concerned.
55. Sending an email involves composing it, addressing it, transmitting it to one or more remote servers, and finally the recipient(s) logging into a server to retrieve and transmit the message to their computer.
56. In general, you should not include confidential information in any email. If you must do so, you must use a secure system, as described below.
57. You must never include person-identifying information in the subject field of an email.
58. You must always take care to ensure that messages are properly addressed to the intended recipients. Think very carefully when using group email addresses. Remember that it is a simple matter to breach confidentiality in the most secure of systems if you send a confidential message to the wrong recipient.
59. The transmission of email from sender to recipients is by default insecure. That is, the message is not encrypted but sent in plain text across networks of indeterminate security. It is a trivial matter to read emails in transit, and in some cases to read users' passwords as they login to their servers.
60. A secure email system is one in which all transmissions between individuals' computers and intervening servers or relays is automatically encrypted, as are the exchange of passwords during a login process. However, although the data is encrypted whilst traversing the network, it is not necessarily encrypted when stored on intervening servers. For complete security, it is necessary to encrypt all or part of the message before it leaves the sender's computer, and for it to be decrypted by the recipient only after it has been received on his/her computer.
61. A webmail system is an email system in which emails are composed and read within a web browser (for example, Hotmail and GMail). Some, but by no means all, such systems automatically use secure, encrypted transmission methods. It will be secure if the URL starts with 'https://' and/or a padlock appears in the browser's status bar.
62. The Trust's email system has a secure login process but does not use encrypted transmission. On the other hand, the transmission of mail between ORH users occurs only

across the NHS network, which is a closed private network and therefore relatively secure. Email sent to non-ORH recipients may well be transmitted across the Internet, which is open and must be assumed to be insecure.

63. The NHS operates its own secure email service, known as *Contact*. This is mainly a webmail service with encrypted transmission and has the advantage that accounts can be accessed securely from anywhere on the Intranet as well as from NHSNet. It is the NHS's intention that all staff use this for intra-NHS email, though uptake has been slow. There is no guarantee however that emails sent to non-NHS users will be transmitted securely once they have left NHSNet.
64. At the moment therefore, the advice is that confidential information should not be sent by email unless absolutely necessary. The NHS *Contact* email system is suitable for transmission of emails between registered NHS users, but because of the possibility of mis-addressing, highly confidential information should first be encrypted, as described above under *Portable information media*, and then sent as an attachment. This method should also be used if it is necessary to email confidential information to non-NHS users.
65. Note that for the recipient to decrypt the attachment, they will need to know the key/password⁴. Transmitting the key is itself a security risk. Clearly, it must never be transmitted with the message itself, and as email systems are not completely tamper-proof, sending it in a separate email is not ideal. Possibly the safest way is by telephone.

Bulk transfers of information

66. Recent concerns about the large scale loss of personal data by Government departments has prompted the Department of Health to stipulate the following requirements regarding bulk transfers of information, which it defines as a transfer of 50 or more personal records.
67. For transfer by email, the information must be sent as an encrypted attachment, as described above. Encrypted attachments are also required when sending 10 or more records by NHS *Contact* email.
68. Recorded delivery must be used for bulk transfer of paper records by post.
69. Data sent on CD or DVD must be encrypted and either hand delivered or, if sent by post, the envelope must be marked '*Private and confidential for addressee only*'.

Non-bulk transfers of person-identifying information by post

70. When sending person-identifying information of more than 10 records/names etc by *internal* post on paper or CD/DVD, mark the envelope '*Private and confidential for addressee only*'
71. When sending person-identifying information of more than 10 records/names etc by *external* post on paper or CD/DVD, recorded delivery must be used.

⁴ Unless *public/private key encryption* is used. Unfortunately there is no NHS standard for this type of encryption.

Maintenance and disposal of computer hardware

72. The maintenance, repair and disposal of computer equipment that stores or has stored patient information must be completed under conditions of strict security.
73. If maintenance or repair is being carried out internally by a Trust member of staff, it must be explained to the person concerned that it may hold confidential, and they should be supervised whilst logged onto the machine.
74. If the maintenance or repair is carried out by an external provider, either:
 - have the work done on-site and supervise the person who does the work, or
 - if the maintenance is done off-site, then you must notify the ICT Department so that any confidential information can be removed before the computer leaves the Trust or the hard-drive removed.
75. Only certain specific contractors are authorised to handle equipment off site on which Trust information is stored. For details, contact the ICT Department.
76. Ensure that you understand how to completely remove or wipe information from a computer. Deleting a file normally only removes its name from the disk directory, it does not obliterate the file itself, and it may be an easy matter for an unauthorised individual to recover it. Special software is required to completely remove all traces of a file from disk. If you need to do this, contact the ICT Department for assistance.
77. If disposing of an old computer that may have had personal or other confidential information stored on it, please contact the ICT Helpdesk (Extension 22822). The ICT Staff will assist you in destroying any such information before the computer leaves the Trust.

IT risk assessment and disaster recovery plans

78. Risk assessment is a process that is designed to help organisations such as the Trust understand and identify the risks posed by a system or situation. IT Risk assessments are usually carried out by local managers on the systems for which they are responsible. However the ICT department can advise on techniques for risk assessment, if required.
79. Departemnts and directorates are responsible for identifying those systems which are important for their activities and business, and for preparing relevant disaster recovery plans. Back-ups of information are a common form of disaster recovery planning; procedures are detailed within the earlier section on backing up/safe storage of data.
80. For System Managers, more information about this process is contained in the Information Protection: System Managers' Guide. If you have queries, or require further information, please contact the ICT Department.

Conclusion

81. This guidance has aimed to outline procedures and protocols, as well as relevant guidance and legislation that intends to enhance the accuracy, availability and confidentiality of information within the Oxford Radcliffe Hospitals NHS Trust.

82. This guidance is not exhaustive, and if members of staff are unsure about any element of information protection, or are dealing with any issue not addressed within the guidelines, they should contact their manager, the ICT Helpdesk (Extension 22822) or ICT Department for advice before proceeding.

Contact details

Director of Planning and Information; Extension 21608

Caldicott Guardian; Extension 21343

ICT Helpdesk; Extension 22822

ICT Department; Through ICT Helpdesk or e-mail "Information Security Office"

- Trust Security Office: 21731 (non emergency)
- Trust Security: 444 (emergency)
- Medical Records Department: 21621

Authors

Susan Haines, David Dickens & David Hopkins (2000).

Revised 2008 by Chris Bunch.

Version control

Version 3.1 Approved by Trust Board 14th April 2000

Version 4.0d March 2008.

Version 4.0 To Trust Board May 2008

Information protection guidelines and procedures

Staff Summary

1. The Trust is involved in using and managing information at almost every stage of healthcare provision. Much of this information is personal and confidential. The Trust and all Trust staff have legal and professional responsibilities to ensure that the quality and confidentiality of this information is safeguarded.
2. Failure to do so could invoke Trust Disciplinary procedures and may be a Criminal Offence under the Data Protection Act 1998.
3. The three documents *Information Protection Policy, Guidelines and Procedures, Information Protection: System Managers Guidelines, and Confidentiality Policy and Guidelines* outline Trust and staff responsibilities, what is regarded as information, and how it can be protected and confidentiality maintained.
4. *Information Protection Guidelines and Procedures* outlines the laws and NHS guidance that apply to information use and management, as well as setting out the Trust and staff obligations under the Data Protection Act 1998. This handout is a summary of that document.
5. Confidentiality and information protection is *everyone's* business.
6. You must ensure that you have understood the *Information Protection Policy, the Information Protection Guidelines and Procedures, and the Confidentiality Policy and Guidelines* before proceeding with any information activity.
7. Information protection need not be time consuming—most elements stated within the policy are simply common sense or good business practice. Changing passwords regularly, not sharing them, or logging out when you are not using a computer or system might prevent Trust information being compromised. A great deal of distress and lost time can be prevented if information is stored securely and backed-up regularly.
8. If you have any concerns over the use and management of information within the Trust, or require further guidance, you should contact your line manager in the first instance or consult the complete copy of the *Information Protection Guidelines and Procedures*.
9. Copies of the guidelines are available from the Trust Intranet or from the ICT Helpdesk (Extension 22822).
10. If you need further advice, please contact the ICT department via the ICT Helpdesk (Extension 22822).

March 2008