

POLICY/PROCEDURE CONTROL SHEET

<u>Policy/Procedure Title</u>	<i>Confidentiality Policy</i>		
<u>Sponsoring Director:</u>	<i>Ian Atkinson – Director of Information and ICT</i>		
<u>Implementation Lead:</u>	<i>Information Governance Manager</i>		
<u>Impact:</u>	<i>(a) To patients</i>	<i>None</i>	
	<i>(b) To staff</i>	<i>None</i>	
	<i>(c) Financial</i>	<i>None</i>	
	<i>(d) Other</i>	<i>None</i>	
<u>Additional Costs:</u>	<i>(a) Training: N/A</i>	<i>Budget:</i>	
	<i>(b) Implementation: N/A</i>	<i>Budget</i>	
	<i>(c) Capital N/A</i>	<i>Budget</i>	
	<i>(d) Other N/A</i>	<i>Budget:</i>	
<u>Training implications:</u>			
<u>Date of consultation at:</u>	<i>Trust Board</i>		
<u>Alignment</u>	<i>Trust Wide</i>		
<u>Date of Final Version:</u>	<i>May 2003</i>		
<u>Implementation Date:</u>	<i>May 2003</i>		
<u>Date of last review:</u>	<i>May 2004</i>		
<u>Date of next review:</u>	<i>August 2005</i>		
<u>Circulation Date:</u>	<i>May 2003</i>		
<u>Circulated Staff:</u>		Yes	No
	<i>Directors:</i>		
	<i>Directors</i>	✓	
	<i>Medical Staff Committee/SMSF</i>		✓
	<i>Records Guardians</i>	✓	
	<i>General Managers</i>	✓	
	<i>H&S Committee Members</i>		✓
	<i>Heads of Department</i>	✓	

Confidentiality Policy

Contents

1. Management Summary-----	4
2. Introduction -----	4
3. Basic Principles -----	5
4. Keeping Patients Informed -----	6
5. Safeguarding Information -----	7
6. Passing Information for other Purposed or as a Legal Requirement-----	12
7. Appendix A - General Guidance to Staff on Confidentiality-----	16
7.1 Introduction -----	16
7.2 Patients -----	16
7.3 Formal Correspondence with Patients and other Hospitals -----	17
7.4 Receipt of Enquiries about Patients-----	17
7.5 Employees-----	17
7.6 Formal Correspondence with Employees -----	18
7.7 Receipt of Enquiries about Patients-----	18
7.8 Use of Faxcsimile (fax) Machines -----	19
7.9 Commercial in Confidence Issues -----	19
7.10 Relationships with the Media -----	19
Appendix B - Related Documents and Policies-----	21
Appendix C - Glossary of Terms-----	22

1. Management Summary

This document contains the Trusts policy on the confidentiality of patient information and establishes clear guidelines and good practice to maintain this confidentiality. Although the policy is written specifically in relation to patient information the guidelines and practice apply equally to maintaining the confidentiality of information about employees of the Trust.

The policy is based on best practice guidance issued by the Department of Health as well as outlining procedures, which ensure that the Trust and its employees meet their legal obligations surrounding the collection and use of confidential information.

The Trust will ensure that all employees and volunteers receive the General Guidance on Confidentiality contained in Appendix A and that training on confidentiality and related issues is provided as part of the Staff Induction Programme. In circumstances where services are contracted out, this policy will also apply and any contract documentation must specify the arrangements made to ensure that confidentiality is maintained.

As a general rule if there is any uncertainty about the release of personal information the matter should be referred to your Manager. Further advice can be obtained from the Information Governance Department, Director of Information or:

- ***Patient Information - the Caldicott Guardian***
- ***Employee Information - the Director of Human Resources***

Out of normal working hours the matter should be referred to the Senior Manager on-call through the Duty Manager

The Trust's Information Governance Group will review this policy on an annual basis.

2. Introduction

The Trust has a great deal of information that must remain confidential. This information is centred on patients and employees in the form of medical records, research records, personnel and finance records.

This policy is based on patients' expectation that information about them will be treated as confidential. It emphasises the importance of making them fully aware that Trust staff and sometimes staff of other agencies need to have strictly controlled access to such information.

Information about patients is not only essential for the prime task of delivering personal care and treatment it is also necessary for a number of other purposes which include:

- assuring and improving the quality of care and treatment;
- monitoring and protecting public health;
- co-ordinating NHS care with that of other agencies;
- effective healthcare administration and contracting;
- teaching;
- statistical analysis and medical and health services research.

As a consequence information will be seen and used by a number of NHS Professionals and administrative staff, as well as staff of other agencies contributing to the delivery of health care. It is a central tenet of the NHS that everyone working for the NHS is under a legal duty to keep personal information confidential.

This policy reflects many of the procedures that are already established in the Trust and sets out:

- the basic principles governing the use of patient information
- informing patients why information is needed, how it is used and their own rights of access to it
- safeguarding information required for NHS and related purposes
- the circumstances in which information may be passed on for other purposes or as a legal requirement.

3. Basic Principles

In general, and in all walks of life, any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information. This **duty of confidence** is long established at common law, but with proper safeguards, need not be construed so rigidly that when applied to the NHS or related services, there is a risk of its operating to a patient's disadvantage or that of the public in generally.

The collection and use of personal information held on computers or in manual records is safeguarded by the **Data Protection Act 1998**. This places obligations on those who record or use the information while at the same time gives specific rights of access to people about whom information is held. The **Computer Misuse Act 1990** provided legal sanctions against unauthorised access or damage to computerised information.

Patient Information

In this policy the term 'patient information' applies to all personal information about members of the public held in whatever form by or for the Trust. As well as obvious material such as medical records, it includes personal 'non-health' information e.g. a patient's name or address or details of their financial or domestic circumstances.

It is neither practical nor necessary to seek a patient's (or other Informant's) specific consent each time information needs to be passed on for a particular purpose. The public expects the NHS, often in conjunction with other agencies, to respond effectively to its needs, it can do so only if it has the necessary information. **It is an essential feature of the relationship between patients and the Trust that patients are informed of the uses to which information about them may be put.**

Within Barnsley a joint agency approach has been developed to establish a Confidentiality Framework. This framework establishes a commitment to patients and service users and is detailed in the Joint Agency Confidentiality Agreement. A copy of this document can be obtained from the Information Governance Co-ordinator.

The Trust's Caldicott Guardian is responsible for the handling of patient information by Trust staff. This role is undertaken by the Trust's Medical Director to ensure that the highest standards of handling are established and adhered to.

The Trust's Information Governance Group provides assistance and support to the Caldicott Guardian by:

- facilitating the identification and implementation of all information governance initiatives
- monitoring progress and compliance on national, local and statutory targets.

When Information May Be Passed On

In summary, information may be passed to someone else:

- **with the patient's consent**
- **on a 'need to know' basis**
- **the recipient needs the information because he or she is or may be concerned with the patient's care or treatment**
- **the use of the information can be justified for the following wider purposes:**
 - **assuring and improving the quality of care and treatment**
 - **monitoring and protecting public health**
 - **co-ordinating NHS care with that of other agencies**
 - **effective healthcare administration**
 - **teaching**
 - **statistical analysis and medical and health services research**
- **the information is required by statute or court order**
- **passing on the information can be justified for other reasons, usually for protection of the public as detailed in Section 6.**

4. Keeping Patients Informed

All NHS bodies must have an active policy of informing patients of the kind of purposes for which information about them is collected and the categories of people or organisations to which information may need to be passed.

The Trust details this information in patient information booklets with the following wording:

"To provide you with a high standard of medical care we need to keep records of your continuing treatment and progress. This is mainly to help the staff looking after you but sometimes other staff are allowed to use these records for teaching and research. You have a right to have access to these records and this should be discussed with your doctor, nurse or therapist. In certain circumstances a charge will be made for this access.

We use computers to assist in the provision of health care. Information is held in accordance with the Data Protection Act and is used for administration, research and statistical analysis. You have a right to have a copy of the information held about you, requests should be made in writing to the Director of Information at the Hospital, a charge will be made for this access.

All staff who have contact with your records are obliged to maintain confidentiality at all times"

As a general rule patients should be told how information might be used before they are asked to provide it and must have the opportunity to discuss any aspects that are special to their treatment

or circumstances. Advice must be presented in a convenient form and be available for general purposes and before a particular programme of care or treatment begins. There must be special arrangements for people whose first language is not English or who have sight or hearing disabilities

Patient's Right Of Access To Their Own Records

The **Data Protection Act 1998**, which came into force in March 2000, establishes a right of access to all personal information by the individuals (Data Subjects) to whom the information relates. This includes health records. The Data Protection Act 1998 replaces the Access to Health Records Act 1990 on this issue. The Access to Health Records Act now only applies to access to records of the deceased.

The following Data Subject rights are established under the Act:

- right of access (following submission of appropriate fee);
- right to prevent processing which may cause damage or distress;
- right to prevent processing for the purpose of direct marketing;
- rights in relation to automated decision taking;
- right to rectify, block, erase or destroy inaccurate data;
- right to request an assessment by the Information Commissioner.

Access to some or all of a record may be excluded if in the opinion of the appropriate Health Professional, information disclosed would be likely to cause serious harm to the physical or mental health of the patient. Access can also be excluded if information relating to a third party other than the patient would enable the third party to be identified.

The Trust (as Data Controller) will ensure that an appropriate data subject access procedure is established and operated. Monitoring procedures will also be maintained to ensure continuing compliance with the Act.

5. Safeguarding Information

The duty of confidence derives from the personal nature of the information that is recorded. Consequently the following all have responsibilities for protecting information:

- **all NHS bodies and those carrying out functions on behalf of the NHS;**
- **everyone working for or with the NHS;**
- **health professionals;**
- **other individuals or agencies to which information is passed legitimately.**

Relevant legislation and best practice guidance:

The Data Protection Act 1998

The Data Protection Act seeks to protect the use of personal information by Data Controllers. The Trust (as Data Controller) affirms that the principles laid down under the Act and detailed below will be followed during all processing of personal data by the Trust.

The Data Protection Act sets 8 principles for the protection of personal data:

Principle 1: personal data should be processed fairly and lawfully

- Principle 2: personal data shall be obtained and process for one or more specified purposes only
- Principle 3: personal data must be adequate, relevant and not excessive in relation to its specified purpose
- Principle 4: personal data shall not be held longer than is necessary
- Principle 5: personal data should be accurate and be kept up to date
- Principle 6: processing must be in accordance with the rights of the individual
- Principle 7: appropriate technical and operational means should be adopted to protect personal data
- Principle 8: personal data should not be transferred outside of the EU without adequate protection.

The Trust (as Data Controller) will ensure that these principles are followed and that staff, volunteers and contractors are made aware of their liabilities and responsibilities.

The Information Governance Co-ordinator will act as the Data Protection Officer for the Trust and will ensure that all processing of personal data undertaken by the Trust is identified and notified to the Information Commissioner.

All staff are required to supply the Data Protection Officer with details of any new processing of personal information, which might affect the Trust's notification.

Caldicott Principles

The Caldicott report was issued in response to concerns over the use of patient information and the need to retain confidentiality. All NHS Trusts are now required to implement the recommendations and principles from the report for safeguarding confidential information.

The Caldicott report established a nation wide network of Caldicott Guardians with responsibility for overseeing the implementation of confidentiality safeguards. The Medical Director who is supported and assisted by the Information Governance Group undertakes this role within the Trust. Terms of Reference for this group can be obtained from the Information Governance Co-ordinator.

The Caldicott report established six principles that should be followed to protect the confidentiality of patient information. The principles are:

- justify the purpose(s) for using confidential information;
- only use it when absolutely necessary;
- use the minimum that is required;
- access should be on a strict need to know basis;
- everyone must understand their responsibilities;
- understand and comply with the law.

Human Rights Act 1998

Article 8 of the European Convention on Human Rights, which is given effect in UK law by the Human Rights Act, establishes a right to 'respect for private and family life'. It creates a general requirement to protect the privacy of individuals and preserve the confidentiality of their health records. This requirement underpins the framework and guidance contained within the policy.

Health And Care Social Act 2001: Section 60

Section 60 of the Health and Social Care Act 2001 makes it lawful to disclose and use confidential patient information in specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. However, the Data Protection Act 1998 does continue to apply in all circumstances.

The **Health Service (Control of Patient Information) Regulations 2002** were the first regulations to be made under Section 60 of this Act, and support the operations of cancer registries and the Public Health Laboratory Services in respect of communicable diseases and other risks to public health.

Responsibility For Passing On Information

The Trust is accountable for the decisions that are taken to pass on information. These decisions must be taken by the Health Professional responsible for a patient's care and treatment.

Disclosure remains with the professionally qualified person employed by the Trust who is responsible at the time the request is made for the particular aspect of the patient's care. In his/her absence the Caldicott Guardian will be authorised to make the decision in his/her place.

The procedures for handling exceptions vary and advice should be sought where necessary from the Caldicott Guardian. In their absence all disclosure matters should be referred to the Information Governance Department, Director of Information, The Nursing Director or, out of hours, the Senior Manager on-call through the Duty Manager.

Only the minimum identifiable information should be used. Where anonymous or aggregated information would be sufficient for a particular purpose then identifiable detail should be omitted wherever possible.

If a patient wants information withheld from someone who might otherwise have received it in connection with his or her care or treatment, the patient should be informed of any health or social care implications or of other relevant factors and this must be noted. The patient's wishes should be respected unless there are overriding considerations.

If Confidence Is Breached

A breach of Confidentiality 'occurs if anyone deliberately, or by accident, gives information or allows access to information gained through their work to unauthorised persons, without the consent of either the patient or the member of staff to whom the information relates'.

On appointment, all staff will be made aware of their contractual obligations with regard to their duty of confidentiality and a statement to this effect will be included in all employment contracts.

Employees who breach confidentiality will be dealt with through the Trusts Disciplinary procedures and through civil law, if appropriate.

Patients Unable To Give Consent

As the law stands nobody is empowered to give consent on the behalf of an adult. However, if a patient is unconscious or unable due to his or her mental or physical condition to give informed consent or to communicate a decision, decisions to pass on information will in practice usually be taken by the health professionals concerned, taking into account the patient's best interests and, as necessary the views of relatives or carers. Such circumstances will usually arise when a patient has been unable to give informed consent to treatment and/or examination (see Consent Policy – September 2000). An earlier refusal to particular information being passed on, given while a

patient had a capacity to decide, should be respected, unless there are overriding considerations to the contrary.

Children And Young People

The Children's Charter states, 'your child has the right to have access to his/her health records. He or she has a right to know that everyone working in the NHS has by law, to keep those records confidential.'

Young people aged 16 or 17 are regarded as adults for purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults.

Children under 16 who have -the capacity and understanding to take decisions ('Gillick competent') about their own treatment are entitled also to decide whether personal information may be passed on and generally to have their confidence respected. In other instances decisions to pass on personal information may be taken by a person with parental responsibility in consultation with the health professionals involved.

In child protection cases the overriding principle is to secure the best interests of the child. Therefore, if a health professional or other member of staff has knowledge of abuse or neglect it may be necessary to share this with others on a strictly controlled basis so that decisions relating to the child's welfare can be taken in the light of all relevant information.

Security Measures

Physical Security

The Director of Information will ensure arrangements for the adequate security of central filing areas where patient data are stored or accessed. Filing rooms will be locked when unattended and no unauthorised persons will have access to filing rooms.

Offices, which contain patient's records, must be locked when unattended and no unauthorised persons should have access to these offices.

Casenotes must not be left unattended in public areas and care must be taken to keep casenotes secure in patient areas.

Confidential patient or employee information must not be sent in internal transit envelopes. It must be sent in a sealed envelope marked 'Confidential'. Bulky correspondence must always be double wrapped and securely parcelled.

Access to and use of computer systems is subject to compliance with the Trust's Information Security Policy. All staff must be aware of their responsibilities as outlined in the Information Security Policy.

Actual or potential breaches of information security should be reported using the Trust's IR1 form.

Patient records archived to microfilm, microfiche, CD-ROM, magnetic tape and audiovisual equipment must be kept as securely as paper records.

Care should be taken to ensure that unintentional breaches of confidence do not occur by leaving fax machines, computer terminals or Personal Computers unattended.

The transmission and receipt of patient and employee information must only be done in accordance with the Fax Transmission Policy. Staff must refer to this policy before information is sent. Copies of the Policy and associated guidance are available on request from the Information Governance Co-ordinator.

Retention and Destruction of Information

Patient, employee and any other identifiable information will be destroyed after the appropriate retention period in accordance with the relevant Trust Policies (see appendix B).

Records for destruction will be destroyed as confidential waste in accordance with the Trust's Waste Disposal Policy.

Co-ordinating Care With Social Services And Other Agencies

In all areas of health and social care the various agencies involved should aim to deliver a 'seamless' service. Essential patient information must therefore be able to pass between the Trust, local authority social services and other services (such as housing, Education, voluntary or independent bodies) where those agencies are contributing to or planning a programme of care, or where one may need to be initiated. The patient needs to be aware that some information sharing will be necessary and this can be discussed with him or her as part of the care planning process.

If the patient raises any objections, the possible consequences should be explained and assurance given that information will only be shared when the other agencies really need to know. The patient's ultimate decision should be respected unless there are overriding considerations to the contrary.

Within Barnsley the Joint Agency Information Sharing Agreement governs the sharing of information between agencies. Copies of this protocol can be obtained from the Information Governance Co-ordinator.

Patients Who Are Offenders

The Health Care Services for Prisoners, the probation service, police and other criminal justice agencies may be involved in the assessment and care of patients who have committed offences.

This often applies to mentally disordered offenders and others with similar needs, including people seen by the NHS or multi-agency assessment teams before or as the result of a court appearance.

There should be agreed liaison arrangements which ensure the passage of essential information between agencies who are contributing to the patient's care and support which can handle sensitively the passing on of information that may be required by court order or can be justified to protect the public. These arrangements should ensure that information passed on is used only for an authorised purpose.

Patients Receiving Benefits

It has been a requirement that hospital staff notify the Department for Work and Pensions when a patient receiving benefit has been in hospital for four weeks. This is because benefit may have needed to be reduced after six weeks as an inpatient.

The Chancellor's budget statement for 2003 proposed changes to this requirement however no commencement date has yet been agreed. The Information Governance Co-ordinator will update relevant staff once further guidance has been released.

Where information is passed onto the Department for Work and Pensions the patient must be informed.

Protecting Public Health

The surveillance of communicable diseases is essential to maintain high levels of disease prevention, to detect outbreaks and to inform and evaluate immunisation programmes.

This is dependent on the flow of information on a 'need to know' basis between health professionals, microbiologists, Consultants in Communicable Disease Control (CCDC), the Public Health Laboratory Service and Local Authority Environmental Health Officers. Local Authorities have particular responsibilities under the **Public Health (Control of Diseases) Act 1984** and **Public Health (Infectious Diseases) Regulations 1988**.

Certain disease being specifically 'notifiable' by doctor and the 'proper officer' of the authority who is usually the CCDC. Arrangements will be made by the Medical Director to remind staff of these duties annually.

Teaching And Research

Teaching and research into health or disease may benefit existing or future patients, or lead to improvements in public health. Access to personal health data for research purposes by employees or external agencies should not, therefore, be hampered unnecessarily but there must be appropriate safeguards. Although the general rule is that the subject's consent must be obtained for any disclosure of personal health data, in the case of certain kinds of health research this may often not be reasonably practicable, or could be against the subject's own interests.

Access to personal health data for the purposes of research will be determined by the District Research and Ethics Committee, who will obtain formal undertakings that whenever practicable, consent to use the relevant personal health data will be obtained from the health professional originally responsible for that aspect of the patient's health care, or their successor and if there is none, the Trust's Caldicott Guardian.

No approach will be made to a subject about whom data has been disclosed without the consent of the professional currently responsible for the relevant aspect of his health care and/or his General Practitioner.

The personal health data available to the research team will not be disclosed to anyone outside it and will be adequately secured against unauthorised access. No subject will be identifiable from any published results.

All personal health data obtained for the purpose of the research will be destroyed when they are no longer required for that purpose.

Particular Restrictions On Passing On Information

The Trust will not allow personal details of patients to be passed on or sold for fund-raising or commercial marketing purposes.

There are statutory legal restrictions on the disclosure of information relating to patients with **HIV** and **AIDS**, other **sexually transmitted diseases**, **assisted conception and abortion**.

6. Passing Information for other Purposed or as a Legal Requirement

The NHS Plan, launched in July 2000, sets the government's target standards for the NHS in England. This document states the following standards in relation to confidentiality:

- “we will keep any relative or friend you name informed about your condition;
- your health records are confidential and are held securely. You can see your records if you ask. You may be asked if your health records can be used for important health research, including the improvement of care and treatment.
- We will respect your decision”.

Statutory Requirements

In certain instances the Trust or a member of staff may have a statutory responsibility to pass on patient information. **If so, prior consultation with the patient is not required.** However, if the health professional responsible for the patient's care are not those required to pass on the information, the former should be consulted as to whether the clinical facts do indeed mean that disclosure is necessary. If there is any doubt this should be discussed with the Caldicott Guardian and legal advice sought if necessary. The patient and the relevant health care professional should be informed as soon as possible and a note made in the patient's records.

The majority of statutory requirements concern forms of notification, for example births and deaths, communicable diseases, abortion, substance misuse and serious accidents. There are also certain obligations to pass on information under the **Mental Health Act 1983.**

Litigation

The High Court has statutory powers to order the disclosure of documents before and during proceedings for personal injury or death and the production of information to an applicant and his or her legal, medical and professional advisors.

Such orders should specify clearly what information is required and if any aspects are unclear, who should seek clarification and/or legal advice without delay. The health professionals responsible for the patient's care and treatment should be consulted about the disclosure in the case of risk to the patient's care (or someone else's) health. If there is a risk, legal advice should be sought on the possibility of seeking an amendment to the order. Where an order requires

information about a patient who has not instigated a court action, that patient should be notified immediately in case he or she wishes to consider an appeal.

It is a well established practice that at the patient's request, information relevant to legal proceedings may be released, usually to the patient's legal or medical advisor. The information should also be passed to lawyers acting for the NHS body concerned where the action involves the Trust, Health Authority or a member of staff. Where health care matters arise the relevant professional should be informed and, if necessary, given the opportunity to comment. If the patient agrees, information may also be released to a third party involved in proceedings.

Release Of Information To Protect The Public

It may sometimes be justifiable to pass on patient information without consent or statutory authority disclosures for the "discovery of iniquity" are traditionally cited. Most commonly these involve the prevention of serious crime but can extend to other dangers to the general public, such as a public health risk or risk of violence, where, as already noted, essential information may need to be shared with other agencies.

Each case must be considered on its merits, the main criterion being whether the release of information to protect the public should prevail over the duty of confidence to the patient. The possible therapeutic consequences for the patient must be considered whatever the outcome. Decisions will sometimes be finely balanced and may concern matters on which NHS staff find it difficult to make a judgement. It may be necessary to seek legal advice or other specialist advice or to await or seek a court order. It is important not to equate "the public interest" with what may be "of interest" to the public.

Tackling Serious Crime

Passing on information to help prevent, detect or prosecute serious crime may sometimes be justified to protect the public. There is no absolute definition of "serious crime" but section 116 of the **Police and Criminal Evidence Act 1984** identifies some "serious arrestable offence". These include:

treason	murder
manslaughter	rape
kidnapping	certain sexual offences
causing an explosion	certain firearms offences
taking of hostages	hijacking
causing death by reckless driving	
offences under prevention of terrorism legislation	
making a threat, which if carried out would be likely to lead to:	

- serious threat to the security of the state;
- serious interference with the administration of justice or with the investigation of an offence;
- death or serious injury;
- substantial financial gain or serious financial loss to any person.

Passing on information to help tackle serious crime may be justified if the following conditions are satisfied:

- without disclosure, the task of preventing, detecting or prosecuting the crime would be seriously prejudiced or delayed;
- information is limited to that which is strictly relevant to a specific investigation;
- there are satisfactory undertakings that the information will not be passed on or used for any purpose other than the present investigation.

Requests for information relating to a number of patients in order to identify one or more is likely to be justified only if there is a very strong public interest. In all cases the permission of the health professional involved must be obtained and the Caldicott Guardian informed of the intention to disclose information together with the circumstances, in their absence the Information Governance Department, Director of Information, the Nursing Director or, out of hours, the Senior Manager on-call through the Duty Manager.

A record of the disclosure must be kept detailing the circumstances and any advice that was taken.

Press And The Media

The maintenance of good relations with the press and media is important.

In law the same general rules apply to the passing of personal information to the media as in other circumstances the patient's consent must be obtained if he or she is capable of taking a decision. This applies whether or not the patient is a celebrity or public figure.

When a patient is unable to take a decision, the provision of basic information may sometimes be judged to be in his or her best interest. Where possible, relatives should be consulted having regard for their own feelings and possible distress. In all circumstances the Trust must be prepared to justify a decision to release information, which should usually be confined to a brief indication of progress in terms authorised by the relevant health professional.

If a patient or former patient has invited the media to report his or her treatment, the Trust may comment in public but should confine itself to factual information or the correction of any misleading assertions or published comment. The duty of confidence to the patient still applies. If there is any doubt legal advice should be sought.

If a department is contacted by any section of the media, they should initially be directed to the Trust's Head of Communications, who may then pass any questions regarding technical areas of the department such as new equipment, improved services, awards etc. to the department manager.

Any issues relating to legal, hospital or government policy must be referred to the Chief Executive, Director of Information, Nursing Director, Director of Clinical Services or, out of hours, the Senior Manager on-call through the Duty Manager.

A separate procedure exists for dealing with Staff Concerns Regarding Patient Care or the Activities of the Trust (PPRO.PCA1), this is contained in the Trust's Personnel Policies and Procedures Manual.

7. Appendix A - General Guidance to Staff on Confidentiality

7.1 Introduction

- 7.1.1 The principles set out apply to all those working within the Trust, including employees, voluntary workers, staff employed by outside agencies but working on the premises, those employed on unpaid honorary contracts, or those based in the Trust for the purposes of training.
- 7.1.2 Confidentiality is a fundamental right associated with patient care and the employment of staff. Any breach of confidentiality, however innocently made, must be treated seriously. In accordance with the Trust's Disciplinary Rules, breaches of confidentiality will normally lead to summary dismissal.
- 7.1.3 This Guidance is based on the Trust's Confidentiality Policy (Document IG01), which is contained in the Trust's Corporate Governance Manual

7.2 Patients

- 7.2.1 All patients have a right to complete confidentiality in all aspects of their care so that it will be a breach of confidentiality to:
- 7) disclose to an unauthorised person the fact that a patient has been identified as being on the premises;
 - 8) disclose to an unauthorised person any detail about a patient's condition or treatment, or any other detail about a patient learned in the course of working within the Trust;
 - 9) use in any way information learned about patients in the course of working within the Trust for purposes other than those genuinely connected with the Trust's business.
- 7.2.2. An authorised person is a person so defined by an employee's manager.
- 7.2.3 All those working within the Trust must:
- i) not deliberately divulge confidential information concerning patients to unauthorised persons;
 - ii) not discuss confidential information concerning patients in a way which might lead to accidental disclosure in public areas, such as corridors, lift areas, dining or recreational areas within the Trust's premises;
 - iii) not discuss confidential information concerning patients outside the Trust's premises in a way, which might lead to unauthorised persons gaining such information;
 - iv) not use information learned about patients in the course of working within the Trust for their own purposes;
 - v) refer enquiries received from the media, the police, or solicitors, concerning patients to:
 - media - Head of Communications
 - police or solicitors - Chief Executive, Director of Information, Nursing Director or Director of Clinical Services.

Out of hours the Senior Manager on call should be consulted through the Duty Manager. (Existing procedures apply to release of medical records to other parties, the provision of legal reports, etc);

- vi) refer to their manager any situations relating to a possible breach of confidence, about which the employee is unsure.

7.3 Formal Correspondence with Patients and other Hospitals

- 7.3.1 Routine correspondence with patients giving appointments and information must be sent in unmarked envelopes and not franked with the Trust's logo.
- 7.3.2 Medical information, usually in the form of copy Medical Records must be marked "Confidential". Bulky correspondence must always be double wrapped and securely parcelled.

7.4 Receipt of Enquiries about Patients

- 7.4.1 Where requests are received seeking information about patients of the Trust such information will not be disclosed without the express prior permission of the patient. The exceptions to this rule are:
 - i) enquiries received the Department for Work and Pensions acting on behalf of the patient (see Confidentiality Policy – Patients Receiving Benefits)
 - ii) in situations where in the judgement of the Caldicott Guardian of the Trust the failure to release the information would be contrary to the public interest or the interests of the patient concerned. This might include disclosure of information to the police.
- 7.4.2 Where telephone or face-to-face enquiries are received seeking information about patients, the person receiving the enquiry will establish the identity of the enquirer and refer them to the ward, if the patient has been admitted. Patient details must not be released without the express permission of the patient.
- 7.4.3 The only exception is if the caller is from another hospital or GP practice and is seeking information, which may affect the care of the patient. In these situations the identity of the enquirer must be confirmed and if there is any uncertainty with a telephone enquiry, a reply call must be made to confirm the identity of the caller. If there is any doubt this should be referred to your manager. Further advice can be obtained from the Caldicott Guardian.

7.5 Employees

- 7.5.1 All employees of the Trust have a right to complete confidentiality regarding their employment with the Trust, so that it will be a breach of confidentiality to:
 - i) disclose to an unauthorised person the fact that a person is employed by the Trust;
 - ii) disclose to an unauthorised person any detail relating to the person's employment or any other information about an employee learned in the course of working within the Trust;
 - iii) use in anyway information learned about an employee in the course of working within the Trust for purposes other than those genuinely connected with the Trust's business.

7.5.2 An authorised person is a person so defined by the employee's manager or in certain circumstances a person Identified by the employee to whom information may be passed such as banks or building societies requiring status details.

7.5.3 All those working within the Trust must:

- i) not divulge confidential information concerning employees to unauthorised persons. It is accepted that in certain situations in particular where telephone calls are received asking for employees by name that it may be impossible to avoid disclosing the fact that a person works within the Trust. In these situations staff receiving calls should use their discretion or refer to their manager for advice;
- ii) not discuss confidential information concerning employees in a way, which might lead to accidental disclosure in public areas within the Trust's premises;
- iii) not discuss confidential information concerning employees outside the Trust's premises in a way, which might lead to unauthorised persons gaining such information;
- iv) not use information learned about other employees in the course of working within the Trust for their own purposes;
- v) refer enquiries received from the media, police or solicitors, about staff to their manager or the Director of Human Resources;
- vi) refer to their manager or the Director of Human Resources for advice in situations relating to a possible breach of confidentiality about which the employee is unsure.

7.6 Formal Correspondence with Employees

7.6.1 Any correspondence addressed to an employee of the BDGH NHS Trust which is of a personal nature must be marked "Personal and in Confidence"

7.6.2 It is the responsibility of individual members of staff to ensure that any change of address is notified to the Trust on the pro-forma included in weekly/monthly payslips. This information is forwarded to the Payroll Department who notify the Personnel Department of changes on a weekly basis. Staff should in addition notify their manager of any change in address.

7.7 Receipt of Enquiries about Patients

7.7.1 When requests are received seeking information about employees of the Trust. Such information will not be disclosed without the express prior permission of the employee. Financial reference requests from banks, building societies etc. will need to be supported by a signed approval for disclosure from the subject of the reference. If such approval is not available it must be sought before disclosure is made.

The exceptions to this rule are:

- i) enquiries received from the Department of Work and pensions who routinely seek information in relation to benefits e.g. sickness, invalidity, maternity etc;
- ii) in situations where in the judgement of the Director of Human Resources the failure to release the information would be contrary to the public interest or the interests of the employee concerned. This might include disclosure of information to the police.

- 7.7.2 Where telephone or face-to-face enquiries are received seeking to make contact with employees, the person receiving the enquiry will take the name, address and telephone number of the person seeking to make contact and agree to ask the person, if they are employed by the Trust, to contact the person making the enquiry themselves.
- 7.7.3 Where telephone or face-to-face enquiries are received seeking information about employees, the person receiving the enquiry will ask for the request to be made in writing. On receipt of the written request, the express permission of the employee to release the information will be obtained prior to any disclosure in accordance with paragraph 7.1 above.
- 7.7.4 Where switchboard operators receive requests to speak to a named employee of the Trust, they will connect the person making the enquiry to the person concerned. Where they are in any doubt about the legitimacy of the call they will refer the caller to the Personnel Department or, out of hours, the Duty Manager.

7.8 Use of Faxsimile (fax) Machines

- 7.8.1. The transmission and receipt of patient and employee information must only be done in accordance with the Fax Transmission Policy. Staff must refer to this policy before information is sent. Copies of the Policy and associated guidance are available on request from the Information Governance Co-ordinator.

7.9 Commercial in Confidence Issues

- 7.9.1 Employees should be particularly careful of using or making public internal information of a 'commercial in confidence' nature, particularly if its disclosure would prejudice the principles of fair competition. This principle applies whether private competitors or other public sector providers are concerned, and whether or not disclosure is prompted by the expectation of personal gain.
- 7.9.2 More detailed guidance is provided in the Trust's General Policy on Standards of Business Conduct, which is contained in the Trust's Corporate Governance Manual.

7.10 Relationships with the Media

7.10.1 As a representative of the Trust

If a department is contacted by any section of the media, they should initially be directed to the Trust's Head of Communications, who may pass any questions regarding technical areas of the department such as new equipment, improved services, awards etc. to the department manager.

Any issues relating to legal, hospital or government policy must be referred to the Chief Executive, Director of Information, Director of Clinical Services or, out of hours, the Senior Manager on-call through the Duty Manager.

7.10.2 As an employee of the Trust

Employees wishing to raise concerns regarding patient care or the activities of the Trust should follow the 'Procedure for Dealing with Staff Concerns Regarding Patient Care or the Activities of the Trust' (PPRO.PCA1) contained in the Trust's Personnel, Policies and Procedures Manual.

Every reasonable action must be taken to try to resolve issues locally and informally.

The Trust acknowledges the freedom of members of staff to write letters, articles to journals, newspapers, take part in radio and television interviews and demonstrations. However, if staff deal with the media as members of the public, it should be made clear that these are their personal views and they are not speaking, writing or acting as representatives of the Trust. To this end, when participating in demonstrations or television interviews, forms of identification such as badges and ID cards must be removed and BDGH uniforms should not be worn. With regard to radio interviews, or press articles, disclosures should be made indicating that these are personal views.

Appendix B - Related Documents and Policies

Please refer to the Information Governance Policy folder.

Appendix C - Glossary of Terms

Caldicott Guardian

The role of the Caldicott Guardian is to oversee and advise on the implementation of the six Caldicott principles. The Trust's Caldicott Guardian is the Medical Director.

Confidentiality

Data access is confined to those with specified authority to view the data.

Data Controller

A data controller controls the contents and use of a collection of personal data.

Data Subject

Data subjects are usually the person or persons that the Trust holds information about.

Duty of Confidence

Any personal information given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without the consent of the provider of the information.

Health Professional

Professional staff working in health care and registered with and regulated by several statutory bodies.

The Information Commissioner

The information Commissioner enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000. The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and also has an international role.

Information Governance Group

BDGH Information Governance Group is chaired by the Caldicott Guardian and reviews issues surrounding the implementation of the Data Protection Act 1998 and the enforcement of the Caldicott Principles. It also advises the Governance Group of any risk issues.

Informed Consent

Informed consent is where the Trust informs the service user of what will happen to their information and how they will or may use it.

IR1 Form

The IR1 (Incident Reporting) Form is used by the Trust to report any incidents that occur within or related to the Trust. This can include breaches in Security as well as physical accidents etc.

Joint – Agency Confidentiality Agreement

The Joint – Agency Confidentiality Agreement is between the Trust and other non-NHS organisations. The agreement includes guidelines that both organisations must adhere in respect of confidentiality.

Multi – Agency Assessment Teams

An assessment team that includes members from both NHS and non-NHS organisations.

Personal Data

Data consisting of information that relates to a living individual who can be identified from that information (or from that and other information in the possession of the Data Controller) including any expression of opinion about the individual but not any indications of the intentions of the data controller in respect of the individual.

Security Breach

An event that has, or could have, resulted in the loss, damage to NHS assets, or an action that is in breach of NHS security procedures.