Buckinghamshire Healthcare NHS Trust

Information Governance

Confidentiality Code of Practice

Guidelines and Responsibilities when Handling Confidential Personal Information

Version	**8**
Issue	**0**
Approved by	Caldicott and Information Governance Committee
Date Approved	March 2022
Ratified by	Executive Management Committee
Date Ratified	N/A
Author	Information Governance Manager
Lead Director	Director of Strategy and Business Development, acting as SIRO
Name of Responsible Individual/Committee	Caldicott and Information Governance Committee
Consultation	Caldicott & IG Committee
BHT Document reference	BHT Pol 199
Department Document Reference	IG0008
Date Issued	Feb 2022
Review Date	Feb 2025
Target Audience	All Trust staff
Location	CAKE BHT Intranet - Policies, clinical guidelines and SOPs
EIA	N/A

Document History

Version	Details of Changes / Actions / Approval	Status	Author	Date
3.0	Approved following formal review by Trust Management Committee	Approved	A Chilcott	July 09
4.0	Minor amendments, update of document references and amendments to section 3 inclusion of table. Appendix 1 (title and inclusion of introduction), referenced to personally owned, donated or loaned IT equipment. Minor amendment to section 3 (insertion of table) and 4 to reflect appendix 1 name change.	Approved	A Chilcott	May 10
4.1	Minor amendment to section 2 to include reference to information incidents, monitoring and audit	Approved	A Chilcott	Nov 10
4.2	Yearly review -, Additions to Section 2 – Responsibility to provide example of breaches. Minor addition to Appendix A to include reference to not leaving records in vehicles.		A Chilcott	Nov 11
4.3	Draft Formal review – Additions to Section 1 to include reference Common Law Duty of Confidence. New section 4.3 Classification marking of NHS Information. New section 4.4 NHS Care Records Guarantee. New section 10.4.3 – Disclosure of Adoption Information. Minor amendment to Appendix A – Telephone enquiries. Circulated to Caldicott and IG Committee for comments	Draft	A Chilcott	Jan 13
5.0	Approved at Caldicott & IG Chairman's Action and noted at meeting 18.03.13. TMC 29.04.13	Approved	A Chilcott	Mar 13
5.1	Amendment to the Caldicott Principles- addition of 7th principle section 4.2. Added reference to HSCIC new Guide to Confidentiality section 1.		A Chilcott	Dec 13
5.2	Informal review- updated appendix 3 –key contacts, removed names and put contact numbers Section 8 – added 8.5- to include reference regarding consent for people who lack mental capacity, Section 12 – strengthened the section on monitoring		L Pask/ S Abraham	Nov 14
5.2	Approved by Caldicott and IG Committee	Draft	L Pask/ S Abraham	Dec 14
5.2	Approved by Trust Policy & Strategy Group & Ratified by TMC	Approved		Feb 15 March15
5.3	Informal review – modified the section on information left on the telephone answer machine in Appendix 1 under 'Confidential information (patients or staff) must'	Approved by the Caldicott Guardian	L Pask/ S Abraham	Nov 15
5.4	Draft Formal review – Revised section 12 – Monitoring this Code	Draft	L Pask/ S Abraham	May 2016
5.4	Approved by Caldicott and IG Committee Approved by TPSG	Approved	L Pask	June 2016
6.0	Ratified by EMC	Approved	L Pask	July 2016
6.1	Formal review to incorporate the requirements of the new Data Protection Act 2018 and GDPR	Draft	L Pask	Sept 2018
6.1	Caldicott and IG Committee	Approved		Sept 2018
6.1	TPSG	Approved		Sept 2018
7.0	Executive Management Committee	Ratified		Oct 2018

8.0	Formal review – minor addition to Appendix A – Use of mobile phones and digital cameras – to include use of Pando app	Draft		Feb 2022
8.0	Caldicott and IG Committee	Approved		March 2022

Document References

Ref	Document title	Document Reference	Location
1	Information Governance Policy	IG0005	Intranet
2	Information Governance Strategy	IG0041	Intranet
3	IT User Account & Email Usage Policy	IG0035	Intranet
4	Department of Health Confidentiality: NHS Code of Practice	Nov 2003	Intranet
5	Information Disclosure and Sharing Decisions	IG0069	Intranet
6	Procedure for the Release of Person identifiable Data	IG0087	Intranet
7	IT Guidance on the Disposal of Sensitive Data	IG0075	Intranet
8	Policy on the Secure Transportation of Patient Paper Records	MR008	Intranet
9	HSCIC Guide to Confidentiality in health & Social Care	Sept 2013	Internet
10	Mental Capacity Act 2005		Internet
11	Policy for Mental Capacity Act and Deprivation of Liberty Safeguards (DoLs)	BHT POL244	Intranet
12	Policy for the Photography of Patients by Non-Medical Photography Staff	BHT 229	Intranet
13	NHS Digital National Data Opt-out Operational Policy and Guidance Document		Internet
14	Data Protection Policy	IG0117	Intranet
15	Data Protection Act 2018		Internet
16	UK General Data Protection Regulation		Internet
17	IT System Access management Policy	IG0031	Intranet
18	Common Law Duty of Confidentiality		Intranet

Table of Contents

1. INTRODUCTION

Patients entrust the NHS to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect this trust. Therefore, if the legal requirements are to be met and the trust of patients is to be retained, it is essential that the NHS provides, and is seen to provide, a confidential service.

In September 2013, the Health and Social Care Information Centre (HSCIC) also published *"A Guide to Confidentiality in Health & Social Care - Treating confidential information with respect*".

It covers the five confidentiality rules:

1. Confidential information about service users or patients should be treated confidentially and respectfully.
2. Members of a care team should share confidential information when it is needed for the safe and effective care of an individual.
3. Information that is shared for the benefit of the community should be anonymised.
4. An individual's right to object to the sharing of confidential information about them should be respected.
5. Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

This document is a guide to the required practice and responsibility of those who work within or under contract to Buckinghamshire Healthcare NHS Trust concerning the confidentiality of staff and patient information. See the Department of Health guidance *"Confidentiality: NHS Code of Practice" - November 2003.*

The principle behind this Code of Conduct is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust's security systems or controls in order to do so.This document supports the Trust Information Governance Policy IG0005 and should also be read in conjunction with the Trust guidance on Information Disclosure and Sharing Decisions ref: IG0069.

Common Law Duty of Confidence
The Trust must also ensure that it complies with the consent requirements of the Common Law Duty of Confidence (Ref: IG0069 Guidance on Information Disclosure and Sharing Decisions). This means that all patient/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient/client. The patient must be informed of the uses or proposed uses to which their information will be put and they must be given the option to 'opt out' from their information being shared for anything other than direct healthcare purposes. There must also be a clear indication within the health record that the patient has consented or dissented.

2. STAFF RESPONSIBILITY

Every member of staff (including agency, bank, locums, volunteers, non-contract, contracted and student placements) may at some time in the course of their work, handle or have access to

confidential person identifiable information whether relating to patients, their carers, family or friends, staff or any other individuals connected to the Trust.

Staff need to be aware that:

- They are individually responsible for the safekeeping of that information on behalf of the Trust, when it is in their possession.

- They need to apply appropriate levels of information security when handling confidential or sensitive data and in particular the requirement to apply encryption software to any IT portable media used to store or transfer person identifiable data.

- Everyone working for the Trust who records, handles, stores or comes across information that could identify a patient has a Common Law Duty of Confidence to that patient and to the Trust.

- They will have signed a contract of employment that includes a statement of the need to maintain absolute confidentiality of personal information.

- Professional obligations of confidentiality must be applied.

- Unauthorised disclosure/access or misuse of personal data or IT systems is a breach of Trust policy and may constitute a criminal offence. All incidents of this nature will be fully investigated and may lead to disciplinary action in line with the Trust disciplinary procedure and could ultimately lead to dismissal (Ref IG0031 IT System Access Management Policy). For e.g.

  - staff accessing their own personal staff or health records or the records of colleagues, family, friends or others where there is no legitimate business relationship or where access is deemed inappropriate or is not authorised as a specific business purpose

  - sharing of personal logins e.g. passwords/ smartcards etc. or gaining access to systems via another person's login details, whether accidental or deliberate.

  - disclosure/sharing of confidential information where there is no legitimate business relationship or specific business purpose or has not been disclosed on a "need to know basis" e.g. selling of information for personal gain, general indiscretion or "gossip"

- The obligations of confidentiality also apply to confidential organisation/business information

- The Trust information systems are regularly monitored and audited for the following:

  - any failed attempts to access confidential information

  - repeated failed attempts to access confidential information

  - successful or attempted access of confidential information where there is no legitimate business relationship and/or access is deemed inappropriate and/or is not authorised as a specific business purpose

- evidence of shared login sessions/passwords/smartcards etc.

Everyone working for the Trust has a responsibility to comply with Trust policy and the statutory acts that affect the processing and handling of information, confidentiality, the use of systems, and the protection of software and data. These are specifically:

- UK General Data Protection Regulation
- The Data Protection Act 2018
- The Computer Misuse Act 1990
- The Copyright, Design and Patents Act 1988
- The Human Rights Act 1998
- NHS Act 2006 – Section 251
- NHS Care Record Guarantee 2005 (Revised 2011)
- The Network and Information system Regulations (NIS Regulations)

Any breach of the Common Law Duty of Confidence, General Data Protection Regulation or Data Protection Act 2018 with specific reference to unauthorised use/disclosure of personal data or failure to safeguard personal data in accordance with Trust policy will be viewed as gross misconduct and may result in serious disciplinary action being taken, up to and including dismissal. Employees could also face criminal proceedings.

3. WHAT IS CONFIDENTIAL INFORMATION?

A duty of confidence arises when one person discloses information to another (e.g. patient to clinician) in circumstances where it is reasonable to expect that the information will be held in confidence. It is a:–

a) legal obligation that is derived from case law

b) requirement established within professional codes of conduct; and

c) must be included within NHS employment contracts as a specific requirement linked to disciplinary procedures

Information should be considered confidential if it can be related in any way to a specific individual.

3.1 All employees are responsible for maintaining the confidentiality of information gained during their employment by the Trust. Confidential information includes:

Person Identifiable information which can include

- Patient/staff name, initials, address, post code, date of birth, sex, telephone number.
- NHS number, NI number and local patient identifiable codes or anything that may be used to identify a patient directly or indirectly i.e. linked with other information which together may identify an individual.
  An example of this may be a rare disease, rare drug treatment or information relating to a very small numbers and within a small population area.
- Pictures, photographs, videos, audiotapes or other images of patients

3.2 Some organisation/business information will also be considered confidential e.g. financial data, commercial in confidence
Information which, if compromised, is likely to:

- adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;
- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;

3.3 Confidential information can be found in a variety of formats including paper, electronic (including portable devices such as laptops, mobile phones, tablets, CDs, DVDs), visual and other versions of information storage media such as digital images and photographs. In addition, it covers oral communications including the use of the telephone and general conversation.

3.4 The terms 'person-identifiable information' and 'person-identifiable data' (PID) are commonly used to mean any data item or combination of items by which a person's identity may be established. An example of person-identifiable data and sensitive data items as defined in the Data Protection Act 2018 are below:

1) Person identifiable data/Information		**2) Sensitive data/Special Categories of data**
One or more pieces of information which can be used along with public domain information to identify an individual		**Information about an individual whose release is likely to cause harm or distress**
• Forename, Surname or Initials		• Physical or mental health conditions
• Date of Birth		• Sexual health/life
• Gender		• Racial, ethnic, religious or similar beliefs
• Address and/or Postcode		• Political opinions/ Trade Union membership
• Occupation		• Offences committed or alleged, criminal proceedings
• Identity Numbers (e.g. NHS, Hospital, National Insurance, Payroll Numbers)		• Financial/bank records, Tax records, benefits/ Pension records, employment/school records, child protection records, vulnerable adult records or social services records and housing records.
• Location data		• Genetic data
• Online identifiers		• Biometric data

Note: These are not exhaustive lists. Departments should determine whether other information they hold should be included in either category

In this context, some key examples of flows of person-identifiable data would include:

- routinely sent correspondence, e.g. discharge letters, employment correspondence

- manually completed forms, e.g. time sheets
- printouts from systems, clinic/theatre listings, budget statements, payroll information
- electronically exchanged data (both structured and unstructured messages)
- telephone communication

In addition to the above, other information such as audio, video or photographs are also deemed as confidential information if an individual can be identified from any facial or physical attribute or piece of data/information.

4. APPLYING GOOD PRACTICE

In writing these guidelines the aim is to comply with the requirements of the UK General Data Protection Regulation (GDPR), Data Protection Act 2018, Caldicott Report 1997 and Caldicott Review 2, 2013, and other associated legislation and guidance dealing with confidentiality and information security.

Good practice should be applied to all areas such as the office, at the reception desk, on the ward, in the outpatient's clinic, in the laboratory, information moving into, out of and around the Trust, see **Appendix 1 – Information Handling Responsibilities** for further information on good practice and staff responsibilities.

5. INFORMING PATIENTS EFFECTIVELY ABOUT THE USES OF THEIR INFORMATION FOR HEALTHCARE PURPOSES

Patients must be made aware that the information they give may be recorded and may be shared, in order to provide them with their care. It may also be used to support clinical audit and other work to monitor the quality of care provided. Consider whether patients would be surprised to learn that their information was being used or shared in a particular way – if so, they have not been effectively informed (see Fair processing Notice/Privacy Notice on the Trust website).

In order to inform patients effectively, staff must:

- Direct the patients to the Fair Processing Notice/Privacy Notice on the Trust website in response to queries around data sharing or provide them with 'You and Your medical Records' leaflet.

- make clear to patients when they are or will be disclosing information to others and who these others may be

- check that patients are aware of the choices available to them in respect of how their information may be disclosed or used for purposes other than direct health care and that by the withholding of consent will not affect their healthcare or treatment

- check that patients have no concerns or queries about how their information is disclosed and used

- where possible, answer any queries personally or direct the patient to others who can answer their questions (see Appendix 2 for list of Key Contacts)

- respect the rights of patients and facilitate them in exercising their right to have access to their health records

6. CONSENT

There are situations where the need to obtain consent to collect/disclose information is clear (see 7.1 & 7.2, 9.1 & 9.2 below). In other circumstances, the law may either require or enable disclosure and in these cases seeking consent may not be essential. Section 8 explains in detail how to cope with such situations.

7. WHEN IS CONSENT REQUIRED?

7.1 Explicit or Express Consent *need not be* obtained when:

a) A patient has provided confidential information relating to their medical condition for the purpose of receiving treatment and related services for that condition i.e. "Healthcare Purposes" and, who has been made fully aware (effectively informed) of who will need to see information about them in order to provide treatment and care (see section 6). However, the Trust must also ensure that it complies with the consent requirements of the Common Law Duty of Confidence. This means that all patient/client information held on any media must not normally be disclosed for purposes other than direct healthcare without the consent of the patient/client or legal basis under the Common Law Duty of Confidence such as implied consent with reasonable expectation. The patient must be informed of the uses or proposed uses to which their information will be put and they must be given the option to 'opt out' from their information being shared for anything other than direct healthcare purposes. There must also be a clear indication within the health record that the patient has consented or dissented.

b) Information is being disclosed under Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001). This permits the common law duty of confidentiality to be set aside in specific circumstances for medical purposes where patient consent has not been obtained, and there is no other reliable basis in law to permit the disclosure and use of identifiable patient information.

   Where practicable, patients should be informed of the use.

7.2 Explicit or Express Consent *must be* obtained when:

a) The purpose/use of information changes or could include disclosure outside that deemed as "Healthcare Purposes". For example, consent must be obtained prior to disclosure to or use for research, teaching (excluding local clinical audit/assurance of quality of healthcare provided), supporting the work of chaplaincy departments, police & law courts. Consent requires a positive opt-in and where possible should be obtained in writing.

7.3 Patient Choice

Patients generally have the right to object to the use or disclosure of confidential information that identifies them and need to be made aware of this right.
Sometimes if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and in extremely rare circumstances, that it is not
possible to offer certain treatment options. Patients must be informed if their

decisions about disclosure have implications for the provision of immediate and on-going care or treatment. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

Remember, patients have a right to change their mind about giving, withholding or withdrawing consent at any time. Full explanation must be given to the patient in cases where the withdrawing of consent may not always be possible (i.e. publications – where an article written with prior consent has already been published).

The National Data Opt-out – Sharing Patient Data for Research and Planning Purposes

The National Data Opt-Out allows patients to opt out of their confidential information being used beyond their direct care for certain research and planning purposes. It was introduced on 25 May 2018 in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs. All NHS organisations in England are required to be compliant from 31st March 2022.

It does not apply to data that patients have explicitly consented to share, nor to aggregated or anonymised data; only to the use of confidential data without consent.

Staff that are involved in Planning and Research are required to check with the Business Intelligence Team whether a patient has registered an opt-out or not *Ref: National Data Opt Out Guidance for Staff*.

7.4 Children and Young People

As per the new Data Protection Act 2018, young people aged 13 are presumed to be competent for the purpose of consent and are therefore entitled to the same duty of confidentiality as adults. For example, children have the right to request a copy of their personal data and have the right to request that data processing stops. Children under the age of 16 who have the capacity and understanding to take decisions about their own data are also entitled to make decisions about the use and disclosure of information they have provided in confidence. However, if an older child is not deemed competent to consent to processing or exercising their own data protection rights, then an adult with parental responsibility should be consulted.

7.5 People who lack mental capacity

Mental Capacity Act 2005 has issued guidance and specific procedures where it is evident that the data subject does not have the mental capacity to make an explicit decision to give informed consent as to whether or not to share personal/sensitive information.

The Act sets out five statutory principles that underpin the legal requirements. Principle 4 states that 'any act done, or decision made, for or on behalf of a person who lacks capacity must be done in that person's best interests'.

One should also consider any evidence of the patient's previously expressed preferences, such as an advance statement or decision, the views of anyone the patient asks you to consult, or who has legal authority to make a decision on their behalf, or has been appointed to represent them.

8. SEEKING AND RECORDING CONSENT

8.1 Who is responsible for seeking consent for "Non-Healthcare Purposes"?

Ideally, the senior health professional involved in the care of the patient should seek consent for non-healthcare purposes. The health professional should be supplied with all the necessary supporting information to appropriately inform the patient of the proposed use of their information and to answer any questions or queries arising.

To ensure that consent is appropriately sought the following should be applied:

- Explicit consent should be obtained *prior* to the information being used for other non-healthcare purposes
- consent must be freely given, specific, informed, verifiable, auditable
- consent should be in the form of a statement or by a clear affirmative action. In other cases, the method of obtaining consent should be recorded fully and, where appropriate, witnessed
- consent should be reviewed or further consent sought when:
  a) there is a change or extension to the purpose/use or information flow (i.e. disclosure)
  b) the legal status of the patient changes (i.e. child becomes adult)

Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it, and unless the controller has another legal justification for processing, any processing based on consent alone would need to cease once consent is withdrawn.

9. DISCLOSURE

9.1 Legally Required to Disclose

Some statutes place a strict requirement on clinicians or other staff to disclose information. Care should be taken however to only disclose the information required to comply with and fulfill the purpose of the law (proportionate). If staff have a reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the patient or another person, then they should seek legal advice. Consent of the patient or data subject is not always required but he/she should be informed preferably prior to disclosure, unless, informing the data subject is likely to place them or another person at risk. All disclosures must be recorded.

9.2 Legally Permitted to Disclose

Legislation may also create a statutory gateway that allows information to be disclosed by an NHS body where previously it might have been unlawful to do so e.g. section 115 of the Crime & Disorder Act 1998. This sort of permissive gateway generally stops short of creating a requirement to disclose therefore, common law duty of confidentiality must still be satisfied, as must the Data Protection Act 2018 and any information disclosed, proportionate to the request. Consent of the patient or data subject is not always required but he/she should be informed preferably prior to disclosure, unless, informing the data subject is likely to place them or another person at risk. All decisions to disclose and the basis for those decisions must be recorded.

9.3 Disclosing (Sharing information with others) information with appropriate care

The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form except as originally understood by the confider, without his or her permission.

a. *Follow any established information sharing protocols*.
   NHS organisations should have developed, or be in the process of developing, information sharing protocols that set out the standards and procedures that should apply when disclosing confidential patient information with other organisations and agencies. Staff must work within the conventions of these protocols
b. *Identify enquirers, so that information is only shared with the right people.*
   Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. All efforts should be made to seek official identification. Check also that they have a legitimate right to have access to that information i.e. next of kin, Power of Attorney
c. *Ensure that appropriate standards are applied in respect of e-mails, faxes and post*
   Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be.
d. *Share the minimum necessary to provide safe care or satisfy other purposes.*
   This must clearly be balanced against the need to provide safe care where missing information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole medical file is generally needless and inefficient (for both parties) and is likely to constitute a breach of confidence. The Caldicott Principles should always be applied.

9.4 Legal Restrictions on Disclosure

There are three particular areas where there are legal restrictions on disclosing information and NHS organisations should take the necessary steps to secure any information capable of identifying an individual is not disclosed. These are:-

- **Sexually Transmitted Diseases (STD)**

Existing regulations require that every NHS Trust takes all necessary steps to ensure that any information capable of identifying an individual, obtained by any of their members or employees with respect to persons examined or treated for any sexually transmitted disease (including HIV and AIDS), shall not be disclosed except:

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

- **Human Fertilisation & Embryology**

Disclosure restrictions can also apply to fertilisation and embryo treatments where individuals can be identified. Generally, explicit consent is required, except in connection with the:

  - provision of treatment services, or any other description of medical, surgical or obstetric services, for the individual giving the consent
  - carrying out of an audit or clinical practice; or

- auditing of accounts

- **Disclosure of Adoption Information (Post-Commencement Adoptions) Regulations 2005**
  The Regulations require that adoption agencies keep records on the adopted children they have placed for at least 100 years and place limits on the information that can be disclosed.

9.5 General Guidance
For more detailed guidance on disclosure please refer to the Department of Health: *"Confidentiality: NHS Code of Practice"* - November 2003, Annex B – Confidentiality Decisions, pages 25-28 and Annex C – Index of Confidentiality Decisions in Practice, pages 39-45 together with the supplementary guidance on Public Interest Disclosures – November 2010, available on the Trust intranet.

10. REVIEW OF THIS CODE OF PRACTICE

This code of practice should be subject to review when any of the following conditions are met:

a) The adoption of the code of practice highlights errors and omissions in its content

b) Where other codes of practice issued by the Trust conflict with the information contained

c) Where the knowledgebase regarding interpretation of the legislation evolves to the extent that revision would bring about improvement

d) 3 years from the date of approval of the current version

11. MONITORING THIS CODE OF PRACTICE

Minimum requirement to be monitored	Process for monitoring e.g. audit	Responsible individual to undertake monitoring and production of a report	Frequency of monitoring/ auditing	Responsible individuals receiving the monitoring report and for development of action plan	Responsible committee for review of action plan	Responsible committee for monitoring of action and audit to ensure satisfactory conclusion
Staff data protection and confidentiality knowledge	E-learning and face to face training and assessment	IG Team	On Induction and annual thereafter	IG Manager	Caldicott and IG Committee	Caldicott and IG Committee
Confidentiality and data handling breaches	Notification of incidents via the Datix incident reporting system	IG team	Daily by IG team and quarterly by Caldicott and IG committee	IG Manager	Caldicott and IG Committee, SIRO	Caldicott and IG Committee, SIRO

IG compliance and best practice across the Trust	Confidentiality spot checks and lessons learned through incident reporting	IG team	Regular spot checks across Trust sites	IG Manager	Caldicott and IG Committee	Caldicott and IG Committee
Conformance with DoH&SC, NHS Digital and ICO standards	Data Security and Protection Toolkit	IG team	Twice a year	IG Manager	Caldicott and IG Committee, SIRO	Caldicott and IG Committee, Executive Management Committee (EMC), Audit Committee
Adherence to legal and statutory requirements	Review of policies, procedures and information leaflets, Staff training	IG team	Annually and when there is legislative changes	IG Manager	Caldicott and IG Committee, Trust Policy subgroup	Caldicott and IG Committee, EMC

APPENDIX 1 – INFORMATION HANDLING RESPONSIBILITIES

Introduction
This summary of information handling responsibilities is not a replacement for Trust policies on Information Governance and related matters, or for local workplace procedures, but is a supporting document that you can keep easily to hand. If you have any concerns about the practices you are using and the possibility for a breach of confidentiality, then you should raise these with your line manager and/or an appropriate contact from the list on Appendix 2. Remember the "Golden Rule" on confidentiality which you can use as a test in any situation where you have to use someone else's personal information:

> *"Ask yourself, if this was my personal information, would I do what I am about to do? If the answer is 'no' then you need to consider what alternatives there may be."*

Confidentiality as a key part of patient care
All NHS organisations are bound by the Care Records Guarantee which provides a number of commitments to patients and the public, that their records will be used in ways which respect individual rights and promote health and wellbeing. It is important because good Information Governance will help patients to:

- Be more confident about how the NHS handles their information,
- Feel assured that information about them will only be shared with those who need to know and
- Share information safely and appropriately so they receive the best care.

Taking simple steps to communicate effectively can improve patient care.

- Clearly explain what you want to record, why you need to record it and how personal information will be used.
- Give people clear guidance on how to make any concerns and comments known.
- Make sure that the guidance is accessible by making it available in a variety of formats.
- Explain their rights to confidentiality and how to use them and respect their right to see their records, where appropriate
- If an individual does not want information about them used for a particular purpose, try to respect that wish but make sure that they know what this may mean for them and future care provision

By doing this you will respect the rights of individuals and reassure them that their information is being handled legally.

What is a safe haven?
A safe haven is a term used to explain an agreed set of arrangements that are in place in the NHS to ensure confidential personal information e.g. patient or staff information can be handled safely and securely.

All Trusts are required to put in place procedures for the receipt, storage and transfer of confidential and sensitive information. All methods and media should be considered i.e. phone, fax, electronic, paper, post, whiteboards etc.

Key information security statements

For the continued confidentiality of patient and staff data it is generally expected that no patient or staff identifiable data will be taken for use outside Trust locations or legitimate places of work.

For most purposes, fully anonymising or pseudoanonymising the data will allow it to be used without compromising confidentiality, for research for example.

It is recognised however, that on an exception basis there may be a need for legitimate removal. In these cases the individual must understand the risks involved and must make the decision whether to remove patient identifiable data or to take the safer and more secure form of anonymised or pseudoanonymised option.

Patient records including diaries, work sheets, lists etc. **must never** be left unattended in vehicles or in Trust premises. .

Information on Medical/nursing handover sheets should be kept to the minimum to protect the confidentiality of the patients (surname or initials), If it is necessary to print a handover sheet this should not be removed from the ward and should be shredded or placed in confidential bag at the end of the shift.

Personally owned IT equipment **must not** be used for the processing or storage of person identifiable, confidential or sensitive data. In the event of any requirement to work remotely e.g. from home, explicit authorisation from both the appropriate Asset Manager and IT Services Manager must be obtained and will **only** be authorised once appropriate risk assessments have been satisfied - see Agile Working policy and IT Computer Usage Policy for procedures on IT remote working.

ALL portable IT media e.g. laptops, DVDs, CDs, USB devices/memory sticks or keys containing person identifiable data, regardless of its use **must** be secured using approved industry standard AES 256 encryption software. Exceptions can only be made by the Senior Information Risk Owner (SIRO).

Confidential information (patients or staff) must:

- Not be shared or discussed with, or in the presence of, anyone who does not need to know, or is not specifically authorised to know that information, e.g. not in public place
- Have appropriate control applied to patient information, having regard to professional ethics and patient consent. Applying formal access controls for clinical records and statutory requirements to record keeping, retention and disposal
- Have appropriate control applied over the disclosure on non-patient information e.g. staff, relative, visitors in accordance with statutory requirements
- Not be shared with parties outside the NHS e.g. solicitors, insurance companies, employers, police without the written consent of the individual concerned unless there are specific powers to do so
- Always be stored in a secure location, preferably a room that is locked and in some cases alarmed when unattended

- Only be copied on to portable IT devices/media e.g. laptops, DVDs, CDs, USB devices/memory sticks or keys where a member of staff has legitimate business purpose to do so and that has been approved by the manager and only where the device/media used or the files containing confidential data are encrypted with approved industry standard AES 256 encryption software. Passwords must not be written down or stored with the device. A copy of the data should be stored on the Trust network wherever possible. USB encrypted memory keys should only be used for transient and not permanent data storage
- Must not be taken home or removed from the Trust without specific authorisation, this specifically applies to patient's health records and staff data
- Never be left on telephone answer machines. Patient confidentiality can be breached from messages left on answer phones, resulting in embarrassing or harmful situations arising. Before leaving a message consider the urgency of getting the information to the patient. If it is not urgent and another attempt to speak to the patient can be made, do not leave a message.

  If you feel you have to leave a message, think about what you say, and leave the minimum amount of information – for example, 'Please call (number) to talk about your appointment' (This will be clear to the patient, but ambiguous to anyone else hearing the message.)
- Be anonymised wherever possible
- Always be risk assessed prior to any transfer to ensure adequate security and protection

For all types of records, staff working in areas where personal identifiable records may be seen must:

- Shut/lock doors and cabinets as required
- Adopt a "clear desk" policy where possible
- Always wear Trust identification badges or other authorised identification
- Query the status of strangers or staff that are unfamiliar
- Know who to tell if anything suspicious or worrying is noted
- Not tell unauthorised personnel how the security systems operate
- Not breach security themselves

Paper records must be:

- Formally booked out from their normal filing system
- Tracked if transferred, with a note made or sent to the filing location of the transfer or recorded within the relevant electronic tracking system
- Returned to the primary filing location as soon as possible after use
- Stored securely within the clinic or office, arranged so that the record can be found easily if needed urgently.
- Stored securely when not in use so that contents are not seen accidentally
- Inaccessible to members of the public and not left even for short periods where they might be looked at by unauthorised persons

- Held in secure storage with clear labeling. Protective 'wrappers' used where appropriate, indicating sensitivity – though not indicating the reason
- Disposed of in designated confidential waste bags in accordance with Trust policy on records disposal.

With electronic records, staff must:

- Only use logins/passwords/pin numbers that have been specifically allocated to them to use
- Always log-out of any computer system or application when work on it is finished
- Always lock access to their workstation and not leave a terminal unattended and logged-on and remove any provided access management device such as Smartcards
- Not share logins/passwords/pin numbers with other people. If other staff have a need to access records, then appropriate access should be organised for them – this must not be by using others' access identities
- Not reveal passwords/pin numbers to others
- Change passwords/ pin numbers at regular intervals to prevent anyone else using them
- Avoid using short passwords (use 6-8 characters), or using names or words that are known to be personally associated with them (e.g. children's or pet names or birthdays)
- Always clear the screen of a previous patient's information before seeing the next patient
- Use a password-protected screensaver where possible to prevent casual viewing of patient / staff information by others
- Protect information from the view of others as far as possible, taking particular care when there is a visitor present
- Ensure that unwanted confidential printouts/ information are shredded/torn up where possible and disposed of in confidential waste sacks and in accordance with Trust policy on record disposal.
- Ensure that electronic media such as floppy disc's, CD ROMs and Computer hard drives are disposed of in accordance with IT policy and procedures
- Ensure where appropriate, that portable electronic media e.g. Laptops, DVDs, CDs, USB devices /memory keys or sticks are secured either with hard disk encryption or encryption of files containing any confidential data and that passwords are not written down and stored with the device. Encryption must be approved industry standard AES 256. A copy of the data should be stored on the Trust network wherever possible. USB memory keys should only be used for transient and not permanent data storage.
- Ensure that data is stored securely on the Trust network not on standalone PC's or hard drives C:\ which are at risk to theft or loss

Telephone enquiries should be validated by:

- Taking the calling number, verifying the caller details independently and calling back if necessary. Taking a contact telephone number e.g. main switchboard (never a direct line or mobile telephone number).
- Checking with a line manager if needed, whether they are entitled to the information they request.
- Where a caller is asking about a patient, ask the caller to verify details of the patient i.e. dob, address **but do not provide the details to the caller.** Where possible, ask the patient for consent to discuss their details with the caller. If necessary, call the enquirer back once you

have had an opportunity to discuss with the patient or your line manager. Follow your local departmental Standard Operating Procedure on responding to enquiries.

- Any information disclosed should always be proportionate to a request with patient's consent if possible and on a need to know basis only.

  If the person requesting the information is not known, the following steps must be taken:

  - Confirm the name, job title, department/organisation of the person requesting the information
  - Check whether the information can be provided. If in doubt, tell the enquirer you will call back
  - Provide the information only to the person who has requested (do not leave message)

  Where possible, keep a log of all telephone enquiries and subsequent information disclosure. Record your name, date and the time of disclosure, the reason for it and who authorised it. Also record the recipient's name, job title, organisation and telephone number.

Staff should ensure that general conversation involving discussions about individuals (including telephone) is:

- Wherever possible, undertaken in an area out of earshot of others, preferably in a closed office.
- Not undertaken with anyone who is not authorised to receive the information, including family and friends.
- Restricted to the use of personal identifiers (e.g. hospital number) when in public/reception areas

Confidential information sent via internal post or in internal transit should always be:

- Appropriately addressed to a named recipient, post holder, consultant or legitimate Safe Haven (Trust nominated secure area)
- The original documentation should be retained and only copies sent across site. Where this is absolutely unavoidable, then photocopies should be retained within the department.
- Sealed in an appropriately secure envelope/package based on sensitivity and volume
- Marked accordingly, with "Confidential" or "Addressee Only" as appropriate
- Double checked to ensure correct recipient and correct address
- Tracked in or out and signed for as appropriate

Confidential information sent via external post or in external transit should always:

- Be addressed fully and marked accordingly, with "Confidential" or "Addressee Only" as appropriate.
- Double checked to ensure correct recipient and correct address
- Be sealed in an appropriately secure envelope/package based on sensitivity and volume and using tamper proof seals where practicable and appropriate
- Be sent via an approved carrier such as NHS courier, Internal transport or recorded/special delivery for any confidential information sent in quantity, sensitive in nature or if on portable media e.g. floppy disc, CD Rom. Obtaining a receipt as proof of sending/delivery is advised where possible
- Traced & tracked in or out and signed for as appropriate on receipt

- Have appropriate authorisation for leaving the Trust particularly in the case of patients' health records.

Staff wishing to send or receive confidential patient information via fax:

The use of fax machine in sending information is not permitted within the Trust as it is deemed insecure. However, on rare occasion when there is no other option, then data should only be received into a fax machine and an alternative method sought for sending out.

- Ensure that trust fax machines are placed in secure locations away from areas accessible to the public. As a minimum, fax machines should be safely secured when not in use
- Multi-functional office systems should be secured so that only authorised personnel may use them. e.g. password access controls should be in place

Staff using E-Mail must:

- Ensure the Caldicott Principles are applied (anonymised where possible and the minimum identifiable data necessary) wherever possible e.g. use NHS or hospital number as the only identifier
- Apply added protection by placing the identifiable information in a password protected document and send the password on a separate email or phone the recipient to disclose the password
- Check to ensure that the recipient is authorised to receive the data (be careful of shared mailboxes)
- Double check and take care to ensure that it is sent to the correct person and the correct address is used (use of personal address books is recommended)
- When using NHS.net, check the correct recipient name and the correct organisation have been selected
- Trace and track all appropriate emails

Use of Whiteboards

- Must not be sited in areas that are accessible or can be viewed by the public (but where repositioning is impractical, the boards must contain only the minimum amount of patient detail in order for staff to be able to locate the patient i.e. initials, surname, bed, bay).

Disposal of confidential information

- Confidential paper waste must be disposed of in white/blue confidential waste bags or confidential waste bins provided by the Trust.
- Never throw confidential paper waste into wastepaper bins, even if it has been torn up.
- Confidential information should be shredded/torn up prior to being placed in confidential waste bags
- The bags should be secured prior to collection, with a plastic security tag
- Bags should be kept in a secure office until collection i.e. they should not be left in corridors waiting for collection
- Never dispose of any non-paper items in confidential paper waste bags
- Electronic data must be disposed of by specialist methods via the IT Dept. - contact the IT Services Dept for advice

Use of Mobile Phones/ Digital Cameras

- Personal mobile phone cameras **must not be used** to take clinical records/ images/photographs of patients
- Only Trust owned digital cameras should be used to take photographs. Departmental cameras which remain on site should be used wherever possible however, if used off –site must be kept secure at all times and images downloaded to an appropriate Trust network drive and deleted from the camera as soon as practically possible
- The use of Pando (clinical communication platform) is only sanctioned when imaging is needed urgently to support clinical decision making between teams and colleagues and when there is no medical photographer available to support urgent imaging. Pando app must be used in line with Trust approved SOP and ensuring that all legal obligations, regarding clinical imaging of patients and appropriate records management and availability, are met
- Images/ photographs must only be taken having obtained written consent with full explanation of the scope of use *Ref Policy for the Photography of Patients by Non-Medical Photography Staff.*
- All images photographs taken are clinical records, must be filed in the patients' clinical record and remain the property of the Trust unless explicit consent has been obtained for another specific purpose and of which has been made clear to the patient
- All images/ photographs and cameras must be kept secure at all times (locked away when not in use)
- All images /photographs that are not immediately downloaded must be labeled with an appropriate identifier to enable direct link to the patient
- Cameras should be cleared of all data after each use/session
- Advice should be sought from the Clinical Photography Department on appropriate storage of images and for any further information

APPENDIX 2 – KEY CONTACTS

For further information or advice please contact:

Information Governance Manager	buc.tr.info.gov@nhs.net
Medical Records Manager	Julie.burnham1@nhs.net
Freedom of Information Co-ordinator	bht.bhinfo@nhs.net
Caldicott Guardian	g.kidner@nhs.net
Senior Information Risk Owner (SIRO)	ian.roddis@nhs.net
Data Protection Officer	mark.austin2@nhs.net