University Hospitals of Morecambe Bay NHS Foundation Trust

Document Type: **Policy**	**Unique Identifier:** CORP/POL/015
Document Title: **Confidentiality**	**Version Number:** 5.3
	Status: Ratified
Scope: Trust Wide	**Classification:** Organisational
Author / Title: Helen Speed – Information Systems Manager	**Responsibility:** Innovation, Information and Informatics (I^3) Service
Replaces: Version 5.2, Confidentiality, Corp/Pol/015	**Head of Department:** Steve Fairclough – Chief Information Officer
Validated By: Helen Speed – Information Systems Manager	**Date:** 04/09/2014
Ratified By: Procedural Documents and Information Leaflet Group	**Date:** 22/10/2014
Review dates may alter if any significant changes are made	**Review Date:** 01/12/2017 (Extended – Form 150/2017)

Which Principles of the NHS Constitution Apply? **Please list from principles 1-7 which apply** 3	**Which Staff Pledges of the NHS Constitution Apply?** **Please list from staff pledges 1-7 which apply** 3

Does this document meet the requirements of the Equality Act 2010 in relation to Race, Religion and Belief, Age, Disability, Gender, Sexual Orientation, Gender Identity, Pregnancy & Maternity, Marriage and Civil Partnership, Carers, Human Rights and Social Economic Deprivation discrimination? **Yes**

Document for Public Display: Yes

Reference Check Completed by……Joanne Shawcross……..Date……17.8.16…..…

To be completed by Library and Knowledge Services Staff

Contents

1. BEHAVIOURAL STANDARDS FRAMEWORK

To help create a great place to work and a great place to be cared for, it is essential that our Trust policies, procedures and processes support our values and behaviours. This document, when used effectively, can help promote a workplace culture that values the contribution of everyone, shows support for staff as well as patients, recognises and celebrates the diversity of our staff, shows respect for everyone and ensures all our actions contribute to safe care and a safe working environment - all of which are principles of our Behavioural Standards Framework.

Behavioural Standards Framework – Expectations 'at a glance'

2. SUMMARY

This policy applies to all personal confidential data (PCD) whether written, recorded on a computer, in a visual or audio format or spoken. This policy should be read and understood by all staff including those from non NHS bodies (contractors) who are engaged in Trust business and who receive, record, store or otherwise come across personal data.
This policy informs staff and contractors in the correct procedures for maintaining the confidentiality of personal confidential data.

3. PURPOSE

The NHS is committed to the delivery of a first class confidential service. This means ensuring that all personal confidential data is processed fairly, lawfully and as transparently as possible so that the public can:

- understand the reasons for processing personal confidential data
- give their consent for the disclosure and use of their personal confidential data
- gain trust in the way the NHS handles personal confidential data and
- understand their rights to access personal confidential data held about them

This policy has been written to meet the legal, statutory and regulatory requirements of

- The Data Protection 1998[1]
- The Human Rights Act 1998[2]
- The Computer Misuse Act 1990[3]
- The Copyright Designs and Patents Act[4]
- Confidentiality: NHS Code of Practice[5]
- NHS Records Management Code of Practice[6]
- Access to Health Records 1990[7]
- Crime and Disorder Act 1998[8]
- Freedom of Information Act 2000[9]
- Caldicott Principles[10]

Implementation of this policy will lead to:

Staff understanding their requirements to

- Protect patient information
- Inform patients effectively
- Provide choice to patients
- Monitor and improve personal compliance

4. SCOPE

This policy is for all staff, contractors and third parties who have access to personal confidential data.

5. POLICY

5.1 Duties

The **Chief Executive** has overall responsibility for ensure that confidentiality is maintained at all times and all disclosures conform to policy

The **Chief Information Officer** has responsibility for Informatics Strategy, Information

The **Caldicott Guardian** has responsibility for advising staff and ensure that adequate arrangements are in place to protect personal confidential data

The **Senior Information Risk Owner** owns the organisation's overall information risk policy and risk assessment processes and ensures they are implemented consistently

The **Information Governance / Security Team** have responsibility for maintaining the currency of the policy and providing advice and guidance on requests on issues relating to confidentiality and data protection.

The **Information Governance Steering Group** will ensure that policy is regularly updated, review incidents and lessons learned, receive audits of staff practice and monitor staff uptake of mandatory Information Governance Training.

Line Managers are responsible to ensure that members of staff follow all policies relating to confidentiality and maintain standards. This includes external contractors and volunteers that work within the area they are responsible for.

Information Asset Owners and Administrators are responsible for ensuring that all staff understand and apply the principles of the legislative, statutory and regulatory requirements relating to confidentiality, information security and data protection.

All Staff must follow the requirements of this and related policies as well as terms of their employment, their legal and ethical obligations and ensure they meet their own professional codes of conduct in relation to confidentiality (Section 4.3)

5.2 What is Personal Confidential Data?

Personal Confidential Data is a collection of information about an individual from which the identity of the individual may be recognised and the individual would reasonably expect this information to be held confidentially.

Patients and staff entrust to or allow the NHS to gather, record and communicate sensitive information about their health and other matters. This is done in confidence and they have a legitimate expectation that staff respect their privacy and act appropriately and in some circumstances where patients lack competence or are unconscious, to extend this trust. This does not diminish the duty of confidence.

A duty of confidence arises when one person (e.g. a patient) discloses information to another (e.g. a clinician) in circumstances (e.g. consultation) where it is reasonable to expect that the information to be held in confidence, this is derived from case law (common law of confidentiality). A duty of confidence is a legal obligation and a requirement within professional codes of conduct and is included in all NHS employment contracts.

All staff working in the NHS are bound by a legal duty of confidence to protect the personal confidential data they may come into contact with during the course of their work. They are obliged to keep any personal confidential data strictly confidential e.g. patient and employee records. Staff may also come into contact with other information

which, although not relating to a person, should be treated with the same degree of care e.g. budget statements, business intelligence reports.

Table 1: Examples of Personal Confidential Data

Patient		*Staff*	
Surname	Sex	Surname	Sex
Forename	NHS number	Forename	Staff number
Initials	National Insurance Number	Initials	National Insurance Number
Address	Ethnic group	Address	Ethnic group
Date of Birth	Local Identifier (Hospitals No)	Date of Birth	Salary details
Other dates (death, diagnosis)	Telephone No	Postcode	Telephone no
Postcode	Occupation	Occupation	

5.3 Staff Responsibilities

All staff are expected to provide a confidential service and should

- understand their obligations defined in the Confidentiality: NHS Code of Practice[5] "Confidentiality Model" – see section 4.3.1
- consider the Caldicott Principles – 2013[10] – see section 4.3.2
- consider the Health and Social Care Information Centre (HSCIC) Guidance or Confidentiality Rules[11] – September 2013 – see section 4.3.3

5.3.1 Staff Responsibilities when Working with Personal Confidential Data

The "Confidentiality Model" in Confidentiality: NHS Code of Practice[5] sets out 4 main requirements

PROTECT

- Fully aware at all times of their responsibilities regarding confidentiality
- Record personal confidential data accurately and consistently
- Keep personal confidential data private
- Keep personal confidential data physically secure
- Disclose and use personal confidential data with appropriate care
- Challenge and verify where necessary the identity of any person who is making a request for confidentiality information and determine the validity of the their reason for requiring that information

INFORM

- Inform patients effectively, "No surprises" as to how their information is being used
- Check where practicable that literature on confidentiality and information disclosure have been read and understood
- Be clear that personal confidential data is recorded or health records accessed
- Be clear when disclosing information with others
- Check patients are aware of choice in respect of how their information may be used or disclosed
- Check patients have no concerns or worries, answering where practicable questions

and queries
- Respect the rights of patients and facilitate them in exercising their rights to have access to their health record

PROVIDE CHOICE
- Allow patients to decide whether their information can be disclosed or used in particular way
- Ask before personal confidential data is used in a way that does not directly contribute or support delivery of their care
- Respect decisions to restrict the disclosure or use of information , except where exceptional circumstance apply
- Communicate to ensure understanding of implications should they choose to agree or restrict the disclosure of information

IMPROVE
- Participate in mandatory training to inform and update on confidentiality issues
- Participate in audit / review of working practices to identify areas for improvement with regards to patient confidentiality and to implement any improvement measures identified
- Report any actual or suspected breaches of confidentiality to the line manager and via the incident reporting system

It is strictly forbidden for staff to view or disclose any information that
- Relates to their own family, friends, or acquaintances unless they are directly involved in the patient's clinical care
- Relates to their own family, friends or acquaintances employed by the Trust unless they are directly involved in their staff management

Actions of this kind will be viewed as breach of confidentiality and are likely to result in disciplinary action.

5.3.2 Caldicott Principles

Ensuring that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care.

1. Justify the purpose(s)
2. Don't use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

Detailed guidance can be found in Appendix 1

5.3.3 Confidentiality Rules (HSCIC)[11]

Guidance for those processing personal confidential data in the relation to the provision of health or social care activities.

Rule 1 - Confidential information about service users or patients should be treated confidentially and respectfully

Rule 2 - Members of a care team should share confidential information when it is needed for the safe and effective care of an individual

Rule 3 - Information that is shared for the benefit of the community should be anonymised

Rule 4 - An individual's right to object to sharing of confidential information about them should be respected

Rule 5 - Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed

Detailed guidance can be found in Appendix 2

5.4 Best Practice to Provide a Confidential Service

5.4.1 Make Sure Information is Shared with the Right People.

- Check that the caller (telephone or in person) is who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly
- Seek official identification or check identity by calling them back (using an independent source for the phone number)
- Check also that the caller has a legitimate right to have access to that information.
- All possible steps must be taken to ensure that patient information is not divulged over the telephone to anyone without authority. Where relatives telephone on the patient's behalf information should not be divulged without the consent or knowledge of the patient
- Requests for information from the Police should always be referred to the Patient Records manager.
- Requests from the media should always be declined and referred to Trust Communications Team (Trust Communications Lead, c/o Trust HQ, WGH ext. 46685), in all circumstances
- If in doubt, check with a line manager, or person in charge of the patient's care.

5.4.2 Have the Staff or Patient Given Permission (Consent) to the Use and Disclose of their Personal Confidential Data

- Ensure that patients and staff have given their consent to the disclosure of their personal confidential data this being either : -
  - *Implied* - agreement has been signalled by patient behaviour e.g. where a patient has agreed to be referred for treatment, by implication they have also consented to relevant medical information being disclosed to support this process
  - *Explicit or expressed* - obtained when the individual has clearly agreed for information to be disclosed. This is a clear and voluntary indication of preference or choice given verbally or in writing, given freely where the options and consequences have been made clear.
- Any exceptions may require written consent from the individual unless they are unable to provide consent (e.g. they are unconscious), then the health professional in charge of the patient's care must be consulted
- If the purpose is not directly concerned with direct healthcare, do not assume consent, e.g. contracting between healthcare organisations. Explicit consent may be required or an alternative to identifiable data be used e.g. anonymisation or pseudonymisation

- If consent cannot be obtained, yet the public good outweighs issues of privacy, Section 60 of the Health and Social Care Act 2001[12] provides interim power so patient confidential data needed to support clinical audit, record validation and research can be used without the consent of the patient.
- Patients and staff should be aware that their personal confidential data may be made available to other members of the health care team, other aspects of Trust business such as clinical governance or clinical audit or another organisation in provision of their healthcare
- Patients and staff have the right to object to the use and disclosure of their personal confidential data and should be aware of the fact. They should be informed of the implications of objecting, e.g. clinician's may be unable to treat them safely, or provide continuity of care, without having the relevant condition and medical history

5.4.3 Share the Minimum Necessary to Provide Safe Care or Satisfy Other Purposes.

- It should meet the need to provide safe care but not be insufficient that omitting the personal confidential data would cause harm.
- Consider how much information is needed before disclosing. Simply providing the whole medical file is generally needless and inefficient (for both parties) and is likely to constitute a breach of confidence.

5.4.4 Information / Data Sharing Agreements

- Set out standards and procedures that apply when disclosing patient confidential data to other organisations and agencies
- Staff must work within the standards and procedures defined within the agreements

5.5 Transferring / Transporting Personal Confidential Data

Staff must ensure that they transfer and transport personal confidential data in a safe and secure manner as detailed below

5.5.1 Email

- Personal confidential data must not emailed outside of the Trust in 'plain text' it must be encrypted either using password protected documents or using secure email (Egress Switch)
- Remove patient identifiers and minimise the amount of information included in the email, restrict to RTX no and initials internally or restrict to NHS number where RTX is not known or required by recipient of the email
- Only send to recipients who have a legitimate need for the information, check the email address and if necessary send a test email
- Personal confidential data should not be contained in the title or body of an email
- If the email is required to be sent external to the Trust then the above two points must apply and it must be sent by Secure Encrypted email using the Trust's secure email system or from an NHS Mail account to an NHS Mail account. Contact the Information Governance / Security department for more details

5.5.2 Fax

- Remove patient identifiable data from any faxes unless you are faxing to a known secure and private area (Safe Haven)
- Faxes should always be addressed to named recipients
- Always check the fax number to avoid misdialling and ring the recipient to check that

they have received the fax
- If your fax machine stores numbers in memory, always check that the number stored is correct and current before sending sensitive information
- The recipient should be contacted to ensure that they are available to receive a fax and arrangements made for the recipient to confirm that the document has been received

5.5.3 Internal Mail

- All correspondence should be addressed to a named recipient. This means personal confidential data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader
- Should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate

5.5.4 External Mail

- All correspondence should be addressed to a named recipient. This means personal confidential data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation
- All envelopes containing confidential patient information should be clearly and fully addressed and securely sealed. The sender's address should be written on the back of the envelope
- Special care should be taken with personal confidential data sent in quantity, such as case-notes, or collections of patient records on paper, floppy discs or other media. These should be sent by Recorded Delivery or by NHS courier, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor
- Case notes and other bulky material should only be transported in the approved boxes and never in dustbin sacks, carrier bags or other containers. These containers should not be left unattended unless empty, when awaiting for collection they should be in a secure area e.g. ideally locked. The containers are only to be taken and transported by the approved carrier
- Electronic media should be password protected. Advice on how to password protect files is available from the I^3 Service Desk
- Blood samples etc. should also only be transported within the correct authorised containers and should not be left lying around within the GP practice or when they have been delivered to the laboratory

5.5.5 Mobile Devices

- Patient information must only be stored on Trust equipment and not on personally owned mobile devices (laptops, PC or Apple devices) this includes devices that are part of the Trust BYOD (Bring Your Own Device) Scheme
- No information should be kept on the hard drive of PCs due to the risk of theft and potential breach of confidentiality. Files should only be stored on the network where they will be backed up centrally
- Only encrypted memory sticks should be used and patient confidential data should only be transferred if absolutely necessary to memory sticks

5.5.6 Voicemail / Answer Phone Messages

- When leaving voicemail or answerphone messages you must consider confidentiality and leave as little information as possible, for example

  Hello, this is a message for < name>. Could you please phone < number> and speak to < full name>. Thank you.

  For enquiries or appointments

  "Hello, this is a message for <name>. I am calling about an enquiry you made today/yesterday. Could you please phone <number> and speak to <full name>. Thank you
  or
  "Hello, this is a message for <name>. I am calling about your appointment. Could you please phone <number> and speak to <full name>. Thank you
- Always make sure we are acting in accordance with the individuals wishes, where possible ask the individual if they are happy to take calls and for messages to be left or even if they are happy with someone else taking a message or dealing with request, always remember to document this

  Detailed guidance can be found in Appendix 3

5.6 Handling or Storing Personal Confidential Data

5.6.1 Offices and Works Areas

- Access to rooms and offices where information is held need to be controlled. Where possible, doors should be locked with keys or keypads. Any rooms designated as "safe havens" must comply with the safe haven guidance
- Always query the status of strangers

5.6.2 Manual or Paper (e.g. handover sheets, case notes, staff confidential reports)

- Personal confidential data must not be taken off site without authorisation
- All records should be formally booked in and out as part of the Trust's record management
- Track all transfers
- Case notes and all patient information must be stored securely in lockable desk drawers or filing cabinets within rooms which should be locked when unattended. Staff must not leave case notes in boxes or in corridors. Transport arrangements must follow Trust procedures
- Printouts and faxes must not be left unattended and must be filed appropriately and locked when not in use
- Store records closed when not in use

5.6.3 Electronic Devices

- Always log out or lock screens when not in use, never leave unattended and logged in
- Never share login or reveal security measure
- Always clear the screen of previous patient information before seeing another
- Discs, tapes and removable media must not be left unattended and must be filed appropriately and locked when not in use
- Patient information must only be stored on Trust equipment and not on personally owned laptops or home desktop computers

- No information should be kept on the hard drive of PCs due to the risk of theft and potential breach of confidentiality. Files should only be stored on the network where they will be backed up centrally
- Computers must not be transferred between users or disposed of other than through the I^3 Service
- Only encrypted memory sticks should be used and unless absolutely necessary patient identifiable information must not be transferred to memory sticks

5.7 Home Working

- It is sometimes necessary for employees to work at their own home. This must be authorised via an appropriate Senior Manager with the department. If authorised, remember that there is personal liability under the Data Protection Act 1998[1] and your contract of employment for breach of these requirements.

5.7.1 Manual Records

- No records which contain personal confidential data or sensitive data should be taken off site unless authorised to do so
- A record is made of who has taken, why they have taken and when the record will be returned
- Ensure any personal confidential data is in sealed containers prior to them leaving the Trust buildings
- Ensure they are put in the boot of the car or carried on your person while being transported from your work place to your home
- Whilst at home, ensure the records are kept secure and confidential. Other members of family and/or friends/colleagues must not be able to see the content or outside folder of the records
- You should not use personal home computers to process or store other persons records
- Returning records must returned in the secure manner they were transported outside the Trust and the record updated accordingly

5.7.2 Electronic Records

- Must only be taken off site on a Trust encrypted device e.g. Laptop or encrypted memory stick
- Whilst at home, ensure the records are kept secure and confidential. Other members of family and/or friends/colleagues must not be able to see the content of the records
- You should not use personal home computers to process or store other persons records

5.8 Disposal of Personal Confidential Data

All confidential information must be disposed of in a secure and appropriate manner

5.8.1 Paper-based personal confidential data

- Always use ‘Confidential Waste’ bins, sacks or shredders to dispose of personal confidential data
- Keep the waste in a secure place until it can be collected for secure disposal
- If you do not have a ‘Confidential Waste’ bins in your area, contact the Estates and Facilities department to arrange delivery

5.8.2 Computer printouts

- Always use 'Confidential Waste' bins, sacks or shredders to dispose of computer printouts
- Keep the waste in a secure place until it can be collected for secure disposal
- If you do not have a 'Confidential Waste' bins in your area, contact the Estates and Facilities department to arrange delivery

5.8.3 Floppy discs, CDs or DVDs

- Floppy discs, CD or DVDs containing confidential information must be securely destroyed
- Contact the I^3 Service Desk who will advise you regarding secure disposal

5.8.4 Computer Files Stored on the Trust Network

Computer files with confidential information no longer required must be deleted from the server in line with the Trust Record Management Procedure

5.8.5 Computer Hard Disks

Computer hard disks must be destroyed and disposed of by the Trust contracted equipment Disposal Company. The company will dispose of the equipment on Trust premises and will provide a full documentation of the disposal process.

5.9 Breaches of Confidentiality

Any potential or actual breaches of confidentiality must be reported to the member of staff's line manager, Information Governance / Security department and recorded on the incident management system.
An investigation will be conducted, either by the line manager or in conjunction with Information Governance / Security and will reported to the appropriate governance committee. This may result in the matter being treated as a disciplinary offence under the organisations disciplinary procedure and may also be reported to Department of Health and Information Commissioner's Office (ICO). Breaches reports to the ICO may result in the organisation being ordered to pay up to £500,000 as penalty for a serious breach of the Data Protection Act 1998[1].

5.10 Contacts

Information Governance	Information.Governance@mbhci.nhs.uk
Information Security	MBHCI.Security@mbhci.nhs.uk
I^3 Service Desk	servicedesk@mbhci.nhs.uk Extension: 46000 or 01524 516000

6. ATTACHMENTS	
Number	**Title**
1	Caldicott Principles
2	Health And Social Care Information Centre Guidance – Confidentiality Rules
3	Guidance on leaving voicemail / answer phone messages
4	Equality and Diversity Impact Assessment Tool

7. OTHER RELEVANT / ASSOCIATED DOCUMENTS	
Unique Identifier	**Title and web links from the document library**
Corp/Pol/116	Acceptable use policy for information communication and technology (ICT) systems and equipment http://uhmb/cs/tpdl/Documents/CORP-POL-116.docx
Corp/Pol/052	Clinical records management policy http://uhmb/cs/tpdl/Documents/CORP-POL-052.docx

8. SUPPORTING REFERENCES / EVIDENCE BASED DOCUMENTS References in full	
Number	References
1	DoH (1998). Data Protection Act 1998. London: DoH. www.legislation.gov.uk/ukpga/1998/29 (accessed 17.8.16)
2	DoH (1998). Human Rights Act 1998. London: DoH. www.legislation.gov.uk/ukpga/1998/42 (accessed 17.8.16)
3	DoH (1990). Computer Misuse Act 1990. London: DoH. www.legislation.gov.uk/ukpga/1990/18 (accessed 17.8.16)
4	DoH (1988). Copyright, Designs and Patents Act 1998. London: DoH. www.legislation.gov.uk/ukpga/1988/48 (accessed 17.8.16)
5	DoH (2003). Confidentiality: NHS Code of Practice. London: DoH. www.gov.uk/government/publications/confidentiality-nhs-code-of-practice (accessed 17.8.16)
6	DOH (2006). Records Management: NHS Code of Practice. London: DoH https://www.gov.uk/government/publications/records-management-nhs-code-of-practice (accessed 17.8.16)
7	DoH (1990). Access to Helath Records Act 1990. London: DoH. www.legislation.gov.uk/ukpga/1990/23/pdfs/ukpga_19900023_en.pdf (accessed 17.8.16)
8	DoH (1998). Crime and Disorder Act 1998. London: DoH. www.legislation.gov.uk/ukpga/1998/37 (accessed 17.8.16)
9	DoH (2000). Freedom of Information Act 2000. London: DoH. www.legislation.gov.uk/ukpga/2000/36/pdfs/ukpga_20000036_en.pdf (accessed 17.8.16)
10	DoH (2013). Information: To Share or not to Share. London: DoH. www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF (accessed 17.8.16)
11	Health and Social Care Information Centre (hscic) (2013). A guide to confidentiality in health and social care. HSCIC. www.hscic.gov.uk/media/12822/Guide-to-confidentiality-in-health-and-social-care/pdf/HSCIC-guide-to-confidentiality.pdf (accessed 17.8.16)

12	DoH (2001). Health and Social Care Act 2001. London: DoH. www.legislation.gov.uk/ukpga/2001/15/pdfs/ukpga_20010015_en.pdf (accessed 17.8.16)

9. DEFINITIONS / GLOSSARY OF TERMS	
Abbreviation or Term	**Definition**
Confidentiality	can be defined as 'protecting information from unauthorised disclosure". The British Medical Association (BMA) defines confidentiality as the "principle of keeping secure and secret from others information given by or about an individual in the course of a professional relationship".
Person Identifiable Information	is defined as all items of information with relate to an attribute of an individual should be treated as potentially capable of identifying patients and hence should be appropriate protect to safeguard confidentiality" (Caldicott Committee Report on the Review of Patient Identifiable Information 1997). This also relates to staff.
Information Format	this list is not exhaustive but includes • Paper records such as medical notes, employees records etc. • CD, computer file, printout, DVD photograph or even word of mouth • Information stored on portable devices such as laptops, palmtops, mobile phones and digital cameras • Audit papers • Trust information about its own working such as meeting papers, incident report forms etc. Verbal such as conversations
Anonymised Information	does not identify an individual directly and which cannot reasonably be used to determine identification. Anonymisation requires the removal of name, address, full postcode, or any other combination of detail that identifies a person
Pseudonomyised Information	refers to data in which the most identifying fields within the record are replaced by pseudonyms or artificial identifiers to disguise the patient identity. Unlike anonymised data, pseudonymisation allows 'reversal' if necessary and for legitimate purposes. It is widely used when patient information needs to be interrogated for 'secondary purposes' but patient identity needs protecting.
Explicit or Express Consent	is obtained when the individual has clearly agreed for information to be disclosed. This is a clear and voluntary indication of preference or choice given verbally or in writing, given freely where the options and consequences have been made clear.
Implied Consent	is in place when agreement has been signalled by patient behaviour e.g. where a patient has agreed to be referred for treatment, by implication they have also consented to relevant medical information being disclosed to support this process
Disclosure	is the divulging of data, or provision of access to data
Unlawful or Inappropriate Disclosure	where information is shared / disclosed without the necessary consent or mechanisms specified in policy

Healthcare Team	includes a range of clinical and social care professionals as well as administrative and medical records staff.

10. CONSULTATION WITH STAFF AND PATIENTS		
Name	**Job Title**	**Date Consulted**
Fiona Prestwood	Informatics Security Officer	
Gail Martin	Informatics Security Projects Officer	
Carol Hogarth	Information Governance Officer	

11. DISTRIBUTION PLAN	
Dissemination lead:	Helen Speed
Previous document already being used?	Yes
If yes, in what format and where?	Trust Procedural Document Library
Proposed action to retrieve out-of-date copies of the document:	Library to remove and replace with document on Trust Procedural Document Library
To be disseminated to:	
Document Library	
Proposed actions to communicate the document contents to staff:	Include in the UHMB Friday Corporate Communications Roundup – New documents uploaded to the Document Library

12. TRAINING

Is training required to be given due to the introduction of this policy? *Yes / No * Please delete as required

Action by	**Action required**	**Implementation Date**

12. AMENDMENT HISTORY				
Version No.	**Date of Issue**	**Page/Selection Changed**	**Description of Change**	**Review Date**
1	December 2006	2.2	Updated types of portable devices Corrected wording to 'company documents/files'	
		Document Title page	Amend title to read 'University Hospitals of Morecambe bay NHS Trust'	
		3.1	Changed Caldicott Guardian name to Mr Peter Dyer	
2	May 07	Policy Title	Change policy title to 'Confidentiality – Code of Practice'	
3	January 09		Review date amended	March 2010
4	July 2010		Policy updated to Trust format	March 2013

4.01	December 2013	All sections	Policy reviewed and revised	
4.02	January 2014	All Sections	Updated to reflect comments from consultation	January 2016
4.2	22 January 2014		Policy approved and ratified Procedural Document Group	22 January 2016
4.3	04 September 2014	All sections	Updated Health Informatics to I^3 and include examples	22 January 2016
5.0	January 2015	Section 4.9	Update to include details around ICO fines	01 September 2017
5.1	August 2016	Section 4.5.6 Appendix 3	Added section for leaving voicemail or answer phone messages and guidance in Appendix 3	01 September 2017
5.2	18/08/2017	Page 1	Review Date extended to 01/12/2017 – form 150/2017	01/12/2017
5.3	04/10/2017	Page 4	BSF page added	01/12/2017

APPENDIX 1: CALDICOTT PRINCIPLES

1. **Justify the purpose(s)**

   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and document, with continuing uses regularly review by an appropriate guardian

2. **Don't use personal confidential data unless it is absolutely necessary**

   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of the flow. The need for the patients to be identified should be considered at each stage of satisfying the purpose(s)

3. **Use the minimum necessary personal confidential data**

   Where use of personal confidential data is considered to be essential, the inclusion of each individual items of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out

4. **Access to personal confidential data should be on a strict need-to-know basis**

   Only the individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used from several purposes

5. **Everyone with access to personal confidential data should be aware of their responsibilities**

   Actions should be taken ensure that those handling personal confidential data – both clinical and non-clinical – are made fully aware of their responsibilities and obligations to respect patient confidentiality

6. **Comply with the law**

   Every use of personal confidential data must be lawful. Someone in the organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements

7. **The duty to share information can be as important as the duty to protect patient confidentiality**

   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

APPENDIX 2: HEALTH AND SOCIAL CARE INFORMATION CENTRE GUIDANCE – CONFIDENTIALITY RULES

Rule 1 - Confidential information about service users or patients should be treated confidentially and respectfully

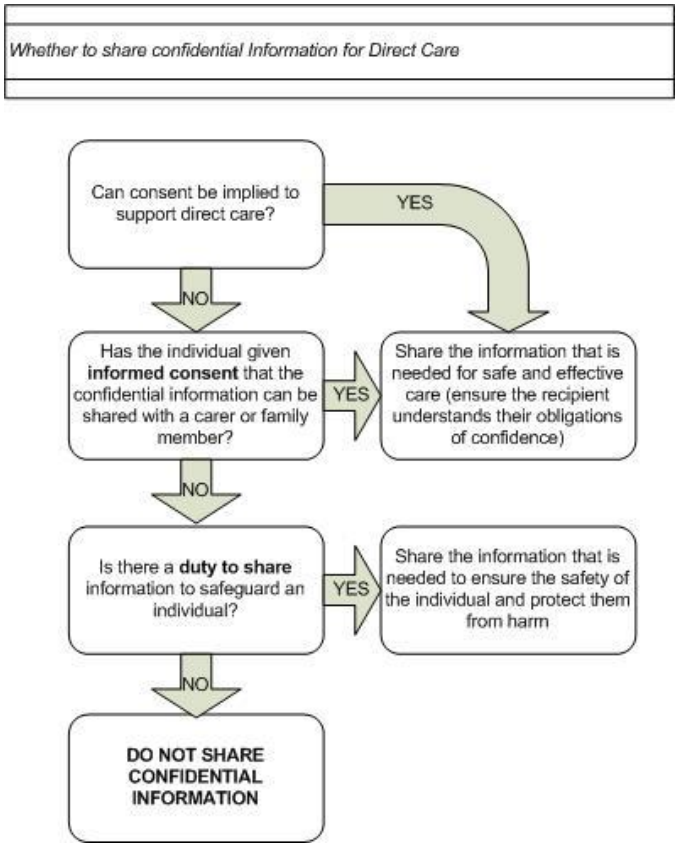
It is right to respect people's privacy and wrong to betray their confidences. Prying and gossip are recognised as unethical in all settings.

- Maintaining trust and respect should always be a priority
- Professional confidentiality obligations should always be respected
- To retain an individual's trust and to support safe care, the care record should be as complete as possible, accurate and fit for purpose

Rule 2 - Members of a care team should share confidential information when it is needed for the safe and effective care of an individual

It is vitally important that health and social care professionals understand they have a duty to share confidential information in the best interests of an individual in their care, when they are providing 'direct care', which is expected to result in better or safer care. Individuals could be put at risk if confidential information is not shared. However, where it is clearly beneficial to share for 'direct care' purposes, confidentiality and privacy still apply. Only those that have a clear 'need to know' should have access to the relevant confidential information.

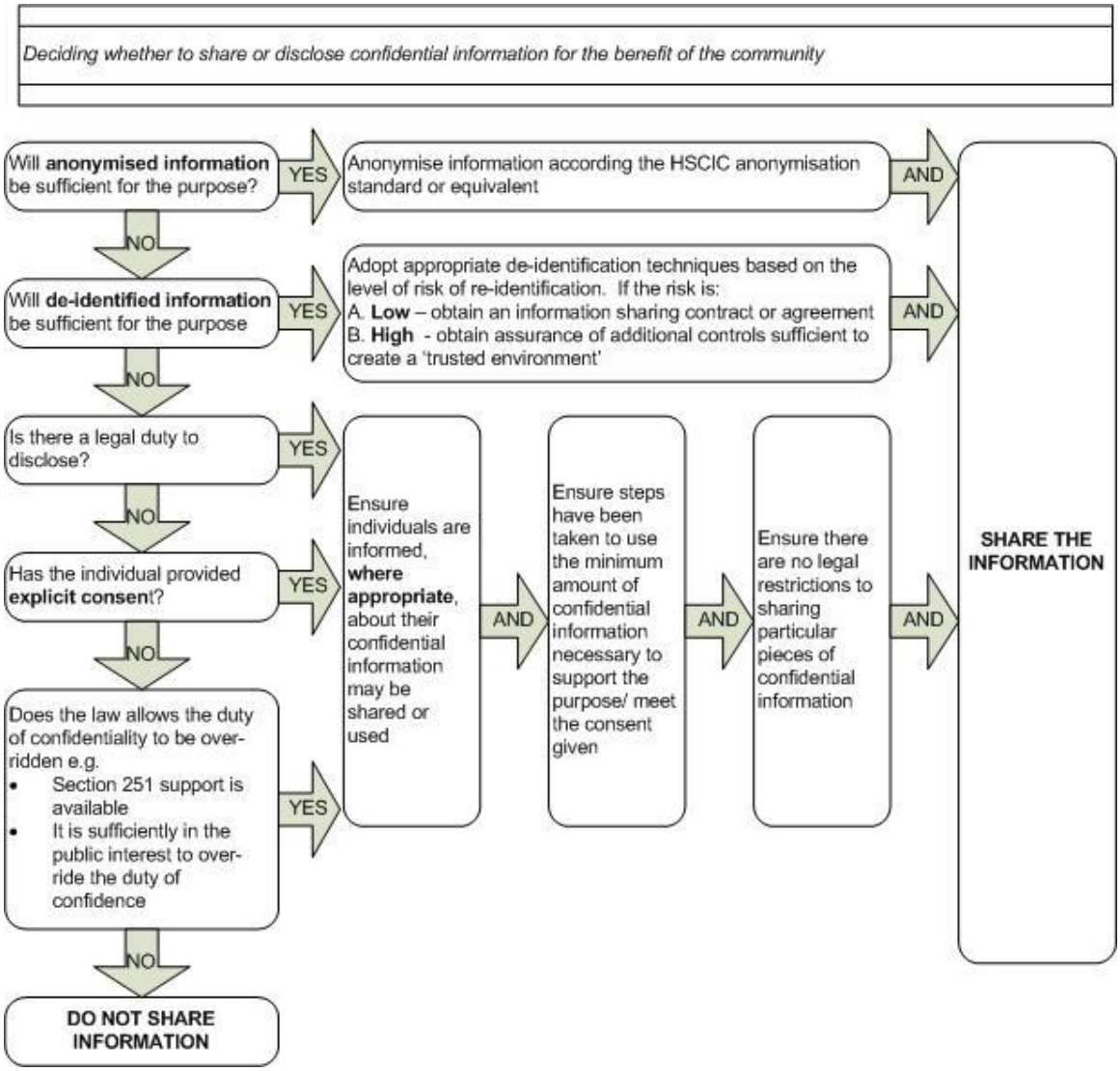
- Confidential information should be shared for safe and effective care
- When confidential information is shared it should be relevant, necessary and proportionate
- However under some circumstances professionals have a duty to share confidential information about individuals in their care



Rule 3 - Information that is shared for the benefit of the community should be anonymised

Where information is for the benefit of the community rather than the support of direct care and to protect individual's confidentiality anonymised information should be used. Information is considered to be anonymised when this is little or no risk of an individual being identified from the information.

- Generally, anonymised information can and should be used to support the improvement of care services
- Sometimes anonymised information by itself is not sufficient to release benefits to the community, occasionally it is important to have information at a service level or patient level to differentiate between individuals e.g. information being linked together using one identifying characteristic but not identifying the individual. The controls required should be based on the risk of re-identification of individuals. The risk could be controlled by data sharing agreements or contracts
- In exceptional circumstances it may be necessary to use confidential information but this requires informed consent of the individual or another legal basis which allows or mandates the sharing



Rule 4 - An individual's right to object to sharing of confidential information about them should be respected

Rule 2 address how to respect the choices of individuals in relation to sharing of their confidential information for direct care purposes. The general principles governing how health and social care organisations should handle objections are

- Objections in all cases should be considered consistently reviewing criteria on a regular for assessing objections on an on-going basis. Members of staff should respect an individual wishes and provide an explanation of the likely consequences to aid an informed decision
- Where individuals object to sharing of confidential information from GP Practices for indirect care, confidential information will not be shared
- Where an objection to sharing of confidential information is implemented, anonymised information can be shared. Anonymised information about service users and patients contributes towards the improvement of services that they and the community benefit from without infringing their privacy or disrespecting their confidentiality wishes
- In rare cases where the likely consequences of an objection pose such a significant risk that the object is lawfully overruled, individuals should receive an explanation of why their objection has been overruled. Such as notifiable diseases, overwhelming public interest, where judged informing an individual may prejudice the purpose of sharing (serious crime committed) or might put someone at risk

Rule 5 - Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed

Organisations should ensure they have appropriate organisational and technical systems security, policies, procedures and staff training and education to ensure that information held and shared securely and appropriately. Each organisation should

- Appoint a senior individual responsible for ensuring the confidentiality rules are followed
- Complete an Information Governance Toolkit Assessment (IGT)
- Ensure that all organisation with which it shares confidential information are committed to following the confidentiality rules
- Encourage people to report concerns that the confidentiality rules have not been followed

APPENDIX 3: Guidance on leaving voicemail / answerphone messages

We all need to consider confidentiality when leaving answer machine messages.
We should give as little information as possible out when we do leave messages.

When leaving a message, it is best to say:

"Hello, this is a message for <name>. Could you please phone <number> and speak to <full name>. Thank you".

Alternatively for enquiries or appointments**;**

"Hello, this is a message for <name>. I am calling about an enquiry you made today/yesterday. Could you please phone <number> and speak to <full name>. Thank you".

or

"Hello, this is a message for <name>. I am calling about your appointment. Could you please phone <number> and speak to <full name>. Thank you

The key is to have a record that we have acted in accordance with the patient's wishes; so when taking initial calls and on first contact, it is always good to ask if they are happy to take calls/for us to leave voicemails/to speak to someone else e.g. partner about the case, and for that to be documented.

APPENDIX 4: EQUALITY & DIVERSITY IMPACT ASSESSMENT TOOL

		Yes/No	Comments
1.	**Does the policy/guidance affect one group less or more favourably than another on the basis of:**		
	• Race	No	
	• Ethnic origins (including gypsies and travellers)	No	
	• Nationality	No	
	• Gender	No	
	• Culture	No	
	• Religion or belief	No	
	• Sexual orientation including lesbian, gay and bisexual people	No	
	• Age	No	
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2.	**Is there any evidence that some groups are affected differently?**	No	
3.	**If you have identified potential discrimination are there any exceptions - valid, legal and/or justifiable?**	No	
4.	**Is the impact of the policy/guidance likely to be negative?**	No	
4a	**If so can the impact be avoided?**	n/a	
4b	**What alternative are there to achieving the policy/guidance without the impact?**	n/a	
4c	**Can we reduce the impact by taking different action?**	n/a	

If you have identified a potential discriminatory impact of this procedural document, please refer it to the HR Equality & Diversity Specialist, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact the HR Equality & Diversity Specialist, Extension 6242.