Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

Reference Number: FOI202223/455
From: Other

Date: 20 February 2023

Subject: Surgical Video Recording

Q1 Are surgical procedures routinely recorded in your trust?

A1 Information not held – surgical procedures are not routinely recorded

Q2 What percentage of Consultant Surgeons routinely record their surgical procedures in your trust?

A2 Information not held - None of the surgeons routinely record their operations

Q3 What platform/software is used in your Trust to a) record and b) store surgical video recordings (if different)? Please provide the name(s), manufacturer(s), and annual cost(s) of the platform/software used by your trust.

A3 Robotic surgeries are recorded onto the Trust's NHS servers. Video images of mini-mitral operations recorded are stored on USB sticks.

Q4 Does your Trust store surgical video recordings on NHS computer systems or does it use a third-party product?

A4 Recordings are stored on the Trust's NHS servers

Q5 Does your trust limit how long surgical video recordings can be stored for?

A5 No

Q6 Are patients undergoing surgical procedures asked explicitly for consent to record their procedure a) as part of their routine care or b) in an additional consent process?

A6 There is a section on the consent form for patients to agree to photography as part of routine care.

Q7 Does the consent to record the procedure explicitly include permission to use the recording for non-clinical purposes (e.g. education, research)?

A7 Consent to record includes use for teaching and educational purposes specifically.

Q8 Are there policies for Consultant Surgeons accessing/using their procedural recordings in your trust? If yes, please supply a copy of your policy.

A8 The Trust does not have explicit policies covering surgical procedural recordings. However, data use, confidentiality and consent are covered in the following policies:

Consent to Examination or Treatment-v31
Health Record Management-v60
Code of Conduct for Handling Personal Data-v40

Q9 Are there policies for patients accessing/using their procedural recordings in your trust? If yes, please supply a copy of your policy

A9 Patients would need to apply for such records under Subject Access Provisions which falls under the *Information Disclosure Policy,* attached.

Q10 Are procedural recordings used for non-clinical purposes (e.g. education, research) in your trust?

A10 No

Q11 Does your trust have a governance policy for the a) recording, b) use, and/or c) storage of surgical video recordings? If yes, please supply a copy of your policy.

A11 As per A8

Code of Conduct for Handling Personal Data

Guidelines

For completion by Author			
Author(s) Name and Title:	Wyn Taylor, Head of Information Governance & Administration		
Scope:	Trust-wide	Classification:	Non-clinical
Version Number:	4.0	Review Date:	21/05/2024
Replaces:	Code of Conduct for Handling Personal Data v3.0		
To be read in conjunction with the following documents:	Data Protection Policy; Information Governance Policy; Information Governance Strategy; Information Disclosure Policy; Information Risk Policy; Information Security Management System (ISMS)		
Document for public display:	Yes		
Executive Lead	Kate Warriner		

For completion by Approving Committee			
Equality Impact Analysis Completed:		Yes	
Endorsement Completed:	Yes	Record of Changes	Yes
Authorised by:	Operational IT Group	Authorisation date:	26/05/2021

For completion by Document Control					
Unique ID No:	TD10(11)	Issue Status:	Approved	Issue Date:	03/06/2021
After this document is withdrawn from use it must be kept in archive for the lifetime of the Trust, plus 6 years.					
Archive:	Document Control		Date Added to Archive:		
Officer responsible for Archive:	IG and Document Control Facilitator				

Contents

Document Statement

Liverpool Heart and Chest Hospital recognises the importance of building and maintaining a strong Information Governance framework, to ensure that personal information it's treated with the utmost respect and care.

The purpose of this document is to provide staff working in Liverpool Heart and Chest Hospital with a set of rules outlining the responsibilities and agreed practices regarding the use of personal data within the Trust. The aim of which it to ensure that all personal data is processed in line the obligations set out in data protection legislation, specifically the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR).

The DPA 2018 sets out the data protection framework in the UK, alongside the UK GDPR. It contains three separate data protection regimes:

- Part 2: sets out a general processing regime (the UK GDPR);
- Part 3: sets out a separate regime for law enforcement authorities; and
- Part 4: sets out a separate regime for the three intelligence services.

Data processing carried out by the Trust falls under Part 2.

This document will set out core standards that all employees of Liverpool Heart and Chest Hospital should adhere to and is intended as an overview of the issues that employees need to be aware of when using personal information of patients, staff or other individuals within Liverpool Heart and Chest Hospital NHS Foundation Trust.

Everyone in the Trust must use the resources available to them in an effective, efficient and timely manner having proper regard to the best interests of the public and patients.

The objectives of this document is:-

- To provide a framework within which the Trust will deliver a first-class confidential service
- To provide guidance to staff on handling and processing confidential patient information fairly, lawfully and transparently

1. Roles and Responsibilities

- **Chief Executive**
  The Chief Executive has overall responsibility for confidentiality in the Trust. As the Trust's accountable officer the Chief Executive is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Confidentiality is the key to this as it will ensure that personal information is appropriately safeguarded at all times.

- **Caldicott Guardian**
  The Trust's Caldicott Guardian is responsible for promoting a culture of confidentiality in the organisation, to act as the "conscience" of the organisation in respect of maintaining patient confidentiality and has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

- **Senior Information Risk Owner (SIRO)**
  The SIRO has responsibility for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist.

- **Data Protection Officer (DPO)**
  Key responsibility is to provide independent risk-based advice to the Trust supporting its decision-making relating to the appropriateness of processing of personal and special category data in line with the requirements of the Data Protection Act.

- **Divisional Heads of Operation/Heads of Department/Managers**
  Are responsible for ensuring that the Code and supporting data protection and information governance policies and guideline standards are built into local processes and that there is ongoing compliance with these requirements

- **All Staff**
  All Trust staff, whether clinical or administrative, have a duty to keep all information confidential. Staff must not access records without authority, discuss personal details in a non-working capacity, or transfer personal information electronically without proper permission and encryption.

  All staff have a confidentiality clause within their Trust contract of employment and confidentiality related responsibilities are clearly stated in the contract. All staff must complete mandatory Information Governance training, also called Data Security and Protection Training.

  Failure to adhere to the responsibilities can result in disciplinary action, termination of a contract, dismissal and in some cases criminal charges.

2. Controlled Document Standards

The duty of confidentiality
Patients entrust us with, or allow us to gather, sensitive personal information relating to their health and other matters as part of seeking treatment. They do so in confidence and they have the legitimate expectation that staff will respect their privacy and act appropriately.

In some circumstances patients may lack the competence to extend this trust or may be unconscious, but this does not diminish the duty of confidence. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, a confidential service.

A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It is generally accepted that information provided by patients or service users to a health or social care service is provided in confidence and must be treated as such so long as it remains capable of identifying the individual it relates to. See Appendix 1: Explanation of terms for examples of patient identifiable personal information.

Staff at Liverpool Heart and Chest Hospital should treat patient information with the utmost respect

and care and should always abide by the protocols in this document and any associated policies.

Confidentiality after death
When an individual has died, information relating to that individual remains confidential under the common law and an ethical obligation to the relatives of the deceased exists. Health records of deceased patients are governed by the provisions of the Public Records Act 1958 and this permits the use and disclosure of the information within them only in limited circumstances. The Access to Health Records Act 1990 governs access to the records and grants a small group of people a statutory right to apply for access. This right of access is negated however if the individual concerned requested that a note denying access be included with the record prior to death.

The Data Protection Act 2018 (DPA 2018) and UK General Data Protection Regulation (UK GDPR)
The DPA 2018 and UK GDPR provide more protection for individuals (data subjects) regarding the processing of their personal data and places more privacy and confidentiality considerations on organisations (data controllers) holding and using their information.

The DPA 2018 and UK GDPR also set out the data protection principles that must be complied with. See Appendix 3 for further details.

(a) Lawfulness, fairness and transparency
(b) Purpose limitation
(c) Data minimisation
(d) Accuracy
(e) Storage limitation
(f) Integrity and confidentiality (security)
(g) Accountability

Fairness and transparency
Data protection law requires that individuals are informed about how their data is processed in concise, transparent, intelligible and easily accessible form (Data Protection Principle 1).

The law also provides specific rights to individuals regarding the processing of the personal data including the right to be informed about how their personal data is used, and when this is provided depends on whether or not the data being processed was obtained directly from the data subject.

To comply with the right to be informed the Trust's privacy notice or fair processing notice is available on its website and in the patient information leaflet 'In Confidence', and includes guidance on how individuals can object to the processing of their data – another right granted to individuals by the law.

Lawfulness

The lawful bases or conditions for processing personal data are set out in Schedule 9 of the DPA 2018 and state that at least one of the following conditions **must** apply whenever personal data is processed. Further detail in Appendix 4:

1. Consent
2. Contract
3. Legal obligation
4. Vital interests

5. Public task
6. Legitimate interests – cannot be used by organisations which are public authorities processing data to perform its official tasks – this includes LHCH performing its duties under the NHS Act 2006.

When processing **special category data** such as health; ethnic origin; religion etc. data controllers need to identify both a lawful basis for general processing **and** an additional condition for processing this type of data. The available bases are detailed in Schedule 10 of the DPA 2018 and are listed below with further detail in Appendix 4. The key conditions available for use by NHS organisations when processing patient personal data are highlighted.

1. **Explicit consent**
2. Employment; social security & protection
3. **Vital interests**
4. Legitimate activities
5. Made public
6. **Legal proceedings**
7. **Substantial public interest**
8. **Medicine**
9. **Public health**
10. **Scientific research**

For the purpose of providing direct health care the lawful bases for processing patient personal data are: Schedule 9 (5) / Article 6 (c) legal obligation and Schedule 10 (8) / Article 9 (h) medicine.

Consent

The DPA 2018 and UK GDPR sets a high standard for consent and provides a specific right for data subjects to withdraw their consent; giving individuals' real choice and control over how their personal information is used.

Consent therefore needs a positive opt-in; explicit consent needs to be a clear and specific statement of consent; the use of pre-ticked opt-in boxes; opt-out boxes or other defaults is banned; and separate consent options must available for different processing activities carried out.

The Trust must demonstrate that consent has been received and must keep clear records to demonstrate this. Consent needs to be clearly distinguishable from other matters, therefore consent requests should be prominent, concise, easy to understand and separate from other terms.

Consent requests should include the following:

- Organisation name
- The name of any third party controllers who will rely on the consent
- The reason the data is being collected
- Details of how the data will be used
- Notification that consent can be withdrawn at any time

Consent procedures must be regularly reviewed to ensure they remain effective and are updated in line with any changes to the processing or the purposes for processing the personal data.

Withdrawal of consent instructions from individuals should be acted on as soon as possible.

Unless the individual can exercise a genuine choice over their information consent is **not** the appropriate legal basis and an alternative lawful basis must be identified.

Human Rights Act provisions

The Act incorporates the European Convention on Human Rights, and rights under the Act are enforceable against public bodies, including NHS and social care organisations.

Article 8 grants to individuals the right to respect for private and family life however in general compliance with Data Protection law and the common law of confidentiality will satisfy requirements of this Act.

NHS Care Record Guarantee

The NHS Care Record Guarantee for England sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. It covers people's access to their own records, controls on others' access, how access will be monitored and policed, options people have to further limit access, access in an emergency, and what happens when someone cannot make decisions for themselves.

More information available on:-
https://digital.nhs.uk/services/registration-authorities-and-smartcards#section-3

Professional Regulators Guidance

Guidance issued by the eight health and social care regulators details specific confidentiality requirements for members, over and above those detailed in this Code of Conduct. Appendix 7 list the professional regulators.

3. Procedure

When can personal data / confidential information be disclosed?

The Trust is legally responsible for the personal information it holds. Care must therefore be taken to ensure that when data is sent to an outside organisation, the purposes for which, lawful basis and the manner in which the information is transferred must be carefully considered.

The Trust's Information Disclosure Policy details the circumstances in which personal data may be transferred. In summary, there is no problem with the information being transferred to organisations involved in the care and treatment of the patient, or where the data is required by legal requirement.

When an individual provides consent for the sharing of information about them for a particular purpose this consent provides a legal basis for that information sharing.

Disclosure of personal data about patients must always be done in line with the Caldicott principles, see Appendix 2 for further details:

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

Responsibility for passing on information

You are responsible for your decision to pass on information. If you are unsure whether to pass on information ask the health professional responsible for the patient's care or a nominated senior manager.

The unauthorised passing-on or disclosure of personal information by any member of staff is a serious matter and may result in disciplinary action in line with the Trust's Disciplinary Procedure.

See the Trust's Information Disclosure Policy for further guidance around disclosure of information.

International transfers

The DPA 2018 and UK GDPR imposes restrictions on the transfer of personal data outside the EU to third countries or international organisations.

Personal data can be transferred where:

- The recipient country has been deemed adequate by the UK Government or the organisation ensures an adequate level of protection or
- The recipient organisation has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. See Appendix 6 for examples of adequate safeguards

For guidance on international transfers contact the Information Governance Team.

Access to health records

The DPA 2018 and UK GDPR provides individuals with the right to see or receive copies of their own medical records. With the authorisation of the clinician in charge of the patient's treatment, the records may be supplied, unless in the opinion of the relevant clinician to supply the records would result in unnecessary harm or distress to the patient or another individual.

Access to health records requests are processed by the Information Governance Team and all requests should be date stamped and forwarded to the team immediately. Refer to the Trust's Information Disclosure Policy for further guidance.

Protecting personal information

The Trust's Information Security Management System (ISMS) policy and procedures provide guidance to all users of Trust information and information systems of their responsibilities and the required security standards to be followed.

The ISMS aims to ensure that IT infrastructure, all paper and digital information assets, including patient information is protected to a consistently high standard from all potentially damaging threats, whether internal or external, deliberate or accidental.

This Code of Conduct and the ISMS outline procedures to ensure that when identifiable data is sent to an outside organisation, the potential risks of confidentiality breaches are minimised.

ISMS Security Standard 1: Information Governance and Safe Haven policy controls details guidance on the transmission of information by various media including fax, post, telephone calls and email in safe haven conditions.

Privacy by design

Under data protection law organisations processing personal data must adopt a 'Privacy by Design' approach to protecting the personal data they process. This means implementing appropriate technical and organisational measures and ensuring that the necessary safeguards are integrated into processing activities at the planning and development stage.

Privacy by design must be adopted as the approach for all projects involving personal data and the Trust's procedures are detailed in the Information Risk Management policy.

Expert advice

If you have any queries about the handling of patient identifiable information or have any issues which you feel need to be raised, then contact the Information Governance Team (infogov@lhch.nhs.uk or ext. 1240/1845) or Head of Information Governance & Administration (ext. 1368).

Queries regarding information and cyber security should be directed to the Cyber Manager (ITSecurity@lhch.nhs.uk).

4. Policy Implementation Plan

This document will be published on the Trust's Policy and Procedures intranet page and will be promoted to all staff during the Trust's recruitment and corporate induction process. Further supporting information will be available to staff on the Information Governance intranet site including a copy of the IG Staff Handbook.

References to this document and associated Information Governance policies and procedures will be written into the terms and conditions of employment contracts with Liverpool Heart and Chest Hospital.

5. Monitoring of Compliance

The Operational IT Group will monitor and review compliance on behalf of the Digital Excellence Committee, which responsible is for the oversight of this Code of Conduct on behalf of the Board.

Analysis of information governance and information security incidents will be used to monitor compliance with the Code of Conduct.

Staff awareness of the Code will be assessed by the Head of Information Governance & Administration through assessment of the staff information governance survey and mandatory IG training compliance.

6. References

- Data Protection Act 2018 and UK General Data Protection Regulation
- EU General Data Protection Regulation - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- Information Commissioner's Office website - https://ico.org.uk/

7. Appendices

APPENDIX 1: Explanation of terms

Bulk transfer: A transfer of data relating to 51 or more individuals.

Caldicott Guardian: a senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing

Care records: care records are personal records. They comprise documentary and other records concerning an individual (whether living or dead) who can be identified from them and relating:

- To the individual's physical or mental health
- To spiritual counselling or assistance given or to be given to the individual or
- To counselling or assistance given or to be given to the individual, for the purpose of their personal welfare, by any voluntary organisation or by any individual who:
    - By reason of the individual's office or occupation has responsibilities for their personal welfare; or
    - By an order of a court has responsibilities for the individual's supervision

This record may be held electronically or in a paper file or a combination of both.

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data controller: the organisation or individual which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing

Data subject: the individual who's personal data is being processed

Direct care: A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

Disclosure: This is the divulging or provision of access to information / data.

Health data: personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

Healthcare purposes: These include all activities that directly contribute to the diagnosis, care and treatment of an individual and the audit/assurance of the quality of the healthcare provided. They do not include research, teaching, financial audit and other management activities.

Health or Social Care Body: A public body which exercises functions in connection with the provision of health services or of adult social care in England.

Identifier: An item of data, which by itself or in combination with other identifiers enables an individual to be identified. Examples include:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, postcode, and their equivalent geographical codes, except for the initial four digits of a postcode if, according to the current publicly available data from the Office for National Statistics and/or the Information Commissioner's Office:
    a. The geographic unit formed by combining all postcodes with the same four initial digits contains more than 20,000 people
    b. The initial three digits of a postcode for all such geographic units containing 20,000 or fewer people are changed to 000
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone numbers
5. Facsimile numbers
6. Electronic mail addresses
7. National Insurance numbers
8. NHS number and medical record numbers
9. Health plan beneficiary numbers
10. Account numbers.
11. Certificate/licence numbers
12. Vehicle identifiers and serial numbers, including licence plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Information Commissioner's Office

Indirect care: Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research.

Information: information is the 'output of some process that summaries, interprets or otherwise represents data to convey meaning.' Data becomes information when it is combined in ways that have the potential to reveal patterns in the phenomenon.

Information governance*:* How organisations manage the way information and data are handled within the health and social care system in England. It covers the collection, use, access and decommissioning as well as requirements and standards organisations and their suppliers need to achieve to fulfil the obligations that information is handled legally, securely, efficiently, effectively and in a manner which maintains public trust.

International organisation: an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries***.***

Legitimate relationship: The legal relationship that exists between an individual and the health and social care professionals and staff providing or supporting their care.

Personal data: Data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Processing: Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data;
- disclosure of the information or data by transmission, dissemination or otherwise making available; or
- alignment, combination, blocking, erasure or destruction of the information or data.

Safe Haven: either a secure physical location or the agreed set of administrative arrangements that are in place within the organisation to ensure confidential personal information is communicated safely and securely.

Special category data: Personal data that relate to more sensitive information about individuals. For example, information about an individual's:
•race; •ethnic origin; •politics; •religion; •trade union membership; •genetics; •biometrics (where used for ID purposes); •health; •sex life; or •sexual orientation

Third countries: countries outside the European Union

APPENDIX 2: Caldicott Prinicples

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 documented, with continuing uses regularly reviewed, 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 that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data**
Only those 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 for several purposes.

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

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

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

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

6. **Comply with the law**

Every use of personal confidential data must be lawful. Someone in each 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 3: Data Protection Principles

(a) Processed lawfully, fairly and in a transparent manner

This means organisations (data controllers) must have a valid lawful basis to process personal data. The lawful basis must be determined **before** processing begins and should be documented. Data controllers are required to maintain Privacy Notices explaining their data processing activities to individuals (data subjects).

(b) **Collected for specified, explicit and legitimate purposes**

Data controllers can **only** collect and use information for defined purposes and care must be taken to ensure that information isn't processed for any other purposes that are incompatible with the initial purposes

(c) **Adequate, relevant and limited to what is necessary**

Excessive personal information should not be collected or held and data controllers must **only** collect the information needed for the defined processing purposes

(d) **Accurate and where necessary kept up to date**

Data controllers must take every reasonable step to ensure that inaccurate data is erased or rectified

(e) **Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed**

Once processing for the initial purpose has ended **and** the minimum retention period has passed data controllers must ensure that personal data is either permanently deleted or de-

personalised (i.e. all identifiers removed from it)

(f) **Processed in a manner that ensures appropriate security of the personal data**
Data controllers must take all suitable measures needed to protect the personal data entrusted to them by their data subjects. Measures include restricting access; setting appropriate access controls; routinely backing up electronic data

(g) **Accountability**
The accountability principle requires organisations to take responsibility for what they do with personal data and how they comply with the other principles. They must have appropriate measures and records in place to be able to demonstrate compliance with data protection law.

Appendix 4: Legal bases or conditions for processing personal data

Personal data:

(a) **Consent**: the individual (data subject) has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract**: the processing is necessary for a contract you have with the individual (data subject), or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation**: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests**: the processing is necessary to protect someone's life.

(e) **Public task**: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests**: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Special category data:

(a) **Explicit consent**: the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) **Employment; social security & protection**: processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by

Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) **Vital interests**: processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) **Legitimate activities**: processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) **Made public**: processing relates to personal data which are manifestly made public by the data subject;

(f) **Legal claims**: processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) **Substantial public interest**: processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) **Medicine**: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) **Public health**: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) **Scientific research**: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Appendix 5: Rights of individuals under the Data Protection law (DPA/UK GDPR)

- Right to be informed
- Right of access
- Right to rectification

- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights relating to automated decision making including profiling

Appendix 6: Adequate safeguards for international transfers

Adequate safeguards may be provided for by:

- a legally binding agreement between public authorities or bodies
- binding corporate rules (agreements governing transfers made between organisations within in a corporate group)
- standard data protection clauses in the form of template transfer clauses adopted by the Commission
- standard data protection clauses in the form of template transfer clauses adopted by a supervisory authority and approved by the Commission
- compliance with an approved code of conduct approved by a supervisory authority
- certification under an approved certification mechanism as provided for in the GDPR;
- contractual clauses agreed authorised by the competent supervisory authority or
- provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority

Appendix 7: Professional regulators

- General Medical Council (GMC) – www.gmc-uk.org
- Nursing and Midwifery Council (NMC) – www.nmc-uk-org
- Health and Care Professions Council (HCPC) – www.hcpc-uk.org
- General Dental Council (GDC) – www.gdc-uk.org
- General Chiropractic Council (GCC) – www.gcc-uk.org
- General Optical Council (GOC) – www.optical.org
- General Osteopathic Council (GOsC) – www.oseopathy.org.uk
- General Pharmaceutical Council (GPhC) – www.pharmacyregulation.org

8. Endorsed By:

Name of Lead Clinician / Manager or Committee Chair	Position of Endorser or Name of Endorsing Committee	Date
Wyn Taylor	Head of IG & Administration / DPO	17/05/2021

9. Record of Changes

Section No	Version No	Date of Change	Description of Amendment	Description of Deletion	Description of Addition	Reason
Cover	4.0	May 2021	Change of job title for author			To align with new job title
Whole document	4.0	May 2021	Reference to GDPR replaced with DPA2018 and UK GDPR or data protection legislation			EU exit
Document statement	4.0	May 2021	Objective moved into document statement section			New controlled document template
Document statement	4.0	May 2021		Reference to fines		Detail not required
2. Controlled document standards	4.0	May 2021	Principles amended to reflect the DPA 2018/UK GDPR Lawfully amended to lawfulness Articles 6 and 9 of the GDPR changed to Schedules 9 and 10 DPA 2018		Accountability principle added	To align with legislation and ICO guide to data protection
3. Procedure	4.0	May 2021	International transfers amended to reflect the change from EU to UK GDPR Expert advice amended to reflect change from IT Security Officer to Cyber Manager			EU exit Change to organisation structure
5. Monitoring of compliance	4.0	May 2021		IG survey removed		No longer carried out following move from IG

						Toolkit to the DSP Toolkit
6. References	4.0	May 2021	Change to reflect change in legislation			EU exit
7. Appendices	4.0	May 2021			Accountability principle added to appendix 3	To align with legislation and ICO guide to data protection

Consent to Examination or Treatment

Policy and Procedure

For completion by Author			
Author(s) Name and Title:	Mr. Paul Modi, Consultant Cardiac Surgeon		
Scope:	Trust Wide	Classification:	Clinical
Version Number:	V3.0	Review Date:	18/06/2023
Replaces:	V3.1		
To be read in conjunction with the following documents:	Incident Reporting Policy; Mental Capacity Act; Correct Site Surgery Policy; GMC Obtaining Consent Procedure; Clinical Nurse Specialist PCI Protocol; Clinical Nurse Specialist Pacemaker Protocol; Vulnerable Adult Policy; Information Policy re Leaflets		
Document for public display:	Yes		
Executive Lead	Dr Raph Perry		

For completion by Approving Committee			
Equality Impact Analysis Completed:		No	
Endorsement Completed:	Yes	Record of Changes	Yes
Authorised by:	QSEC	Authorisation date:	07/05/2021

For completion by Document Control					
Unique ID No:	TR05(08)	Issue Status:	Approved	Issue Date:	05/10/2021
After this document is withdrawn from use it must be kept in archive for the lifetime of the Trust, plus 6 years.					
Archive:	Document Control		Date Added to Archive:		
Officer responsible for Archive:	IG and Document Control Facilitator				

Contents

Document Statement

Patients have a fundamental legal and ethical right to determine what happens to their own bodies. Valid consent to treatment is therefore absolutely central in all forms of healthcare, from providing personal care to undertaking major surgery. Seeking consent is also a matter of common courtesy between health professionals and patients.

1. Roles and Responsibilities

2. Controlled Document Standards

3. Procedure

3.0 What consent is – and isn't

This policy sets out the standards and procedures in the Liverpool Heart and Chest Hospital to ensure that health professionals are able to comply with the Department Of Health Guidance f o r obtaining Consent (www.doh.gov.uk/consent).

The context of consent can take many different forms, ranging from active request by a patient for a particular treatment (which may or may not be appropriate or available) to the passive acceptance of a health professional's advice.

"Consent" is a patient's agreement for a health professional to provide care. Patients may indicate consent non-verbally (for example by presenting their arm for their pulse to be taken), orally, or in writing. For the consent to be valid, the patient must:

- be competent to take the particular decision.
- have received sufficient information to take it.
- not be acting under duress.

In some cases, the health professional will suggest a particular form of treatment or investigation and after discussion the patient may agree to accept it. In others, there may be a number of ways of treating a condition, and the health professional will help the patient to decide between them. Some patients, especially those with chronic conditions, become very well informed about their illness and may actively request particular treatments. In many cases, 'seeking consent' is better described as 'joint decision-making': the patient and health professional need to come to an agreement on the best way forward, based on the patient's values and preferences and the health professional's clinical knowledge.

Where an adult patient lacks the mental capacity (either temporarily or permanently) to give or withhold consent for themselves, no one else can give consent on their behalf. However, treatment may be given if it is in their best interests, as long as it has not been refused in advance in a valid and applicable advance directive.

3.1 Stages for Obtaining Consent

When a patient formally gives their consent to a particular intervention, this is only the endpoint of the consent process. It is helpful to see the whole process of information provision, discussion and decision-making as part of 'seeking consent'.

This process may take place at one time, or over a series of meetings and discussions, depending on the seriousness of what is proposed and the urgency of the patient's condition.

3.1.1 Single stage process

In many cases, it will be appropriate for a health professional to initiate a procedure immediately after discussing it with the patient. For example, during an ongoing episode of care, a physiotherapist may suggest a particular manipulative technique and explain how it might help the patient's condition and whether there are any significant risks. If the patient is willing for the technique to be used, they will then give their consent and the procedure can go ahead immediately. In many such cases, consent will be given orally.

If a proposed procedure is invasive or carries risk, it will be appropriate to seek written consent, and health professionals must take into consideration whether the patient has had sufficient chance to absorb the information necessary for them to make their decision. As long as it is clear that the patient understands and consents, the health professional may then proceed. In Thefaut v Francis Johnson, the judgment highlighted that a simple signature on a consent form is not definitive evidence of an acceptance of risk and that, immediately prior to surgery is not the time or place to start explaining risks for the first time.

3.1.2 Two or more stage process

In most cases where written consent is being sought, treatment options will generally be discussed well in advance of the actual procedure being carried out. This may be on just one occasion (either within primary care or in a hospital out-patient clinic), or it might be over a whole series of consultations with a number of different health professionals. The consent process will therefore have at least two stages: the first being the provision of information, discussion of options and initial (oral) decision, and the second being confirmation that the patient still wants to go ahead. The consent form and the case notes should be used as a means of documenting the information stage(s), as well as the confirmation stage.

Patients receiving elective treatment or investigations for which written consent is appropriate should be familiar with the contents of their consent form before they arrive for the actual procedure, and should have received a copy of the page documenting the decision-making process. They may be invited to sign the form, confirming that they wish treatment to go ahead, at any appropriate point before the procedure: in out-patients, at a pre-admission clinic, or when they arrive for treatment. If a form is signed before patients arrive for treatment, however, a member of the healthcare team must check with the patient at this point whether they have any further concerns and whether their condition has changed.

This is particularly important where there has been a significant lapse of time between t h e f o r m being sgned and the procedure. When confirming the patient's consent and understanding, it is advisable to use a form of words which requires more than a yes/no answer from the patient: for example beginning with "tell me what you're expecting to happen", rather than "is everything all right?"

While administrative arrangements will vary, it should always be remembered that for consent to be valid, the patient must feel that it would have been possible for them to refuse or change their mind.

It will rarely be appropriate to ask a patient to sign a consent form after they have begun to be prepared for treatment (for example, by changing into a hospital gown), unless this is unavoidable because of the urgency of the patient's condition.

3.2 Process for Obtaining Consent.

At the time of Consultation with the Consultant / SpR, the patient will be provided with information pertaining to the diagnosis, natural history of condition and the treatment options including no treatment, as well as potential benefits and risks relating to the procedure.

At this Consultation, the patient will receive all information regarding pre- procedure, post-procedure recovery and discharge.

The SpR understands that if further information is required by the patient in order for them to make informed consent, and the SpR / Nurse Practitioner is unable to provide this information, they will contact the patient's Consultant, and that until this is done, informed consent has not been given.

3.3 Process for Recording Consent

The standard consent form provides space for a health professional to provide information to patients and to sign confirming that they have done so. The health professional providing the information must be competent to do so: either because they themselves carry out the procedure, or because they have received specialist training in advising patients about this procedure, have been assessed, are aware of their own knowledge limitations and are subject to audit (see Section 8.0 for discussion of Who can obtain consent for investigations and /or treatment).

Once the patient has received all the necessary information and is happy with the information given a formal recording of consent will be taken by the patient and Consultant / SpR/ Nurse Practitioner.

A copy of the consent form will be given to the patient for their own personal records

This consent form which details the communications with the patients Consultant / SpR will be filed in the patient's health records until such time as the procedure is performed and thereafter for the life of the medical record.

Confirmation of consent will occur before the procedure is performed by a registered health professional to ensure that the patient is satisfied with all information given throughout the consent process and this should be documented in the patient's electronic record.

Confirmation of consent should occur if the consent form was signed more than 24 hours ahead of the planned procedure. When consent occurs on the day of the procedure or the previous day conformation of consent is not necessary.

3.4 Seeking Consent for Anaesthesia

Where an anaesthetist is involved in a patient's care, it is their responsibility (not that of a surgeon) to seek consent for anaesthesia, having discussed the benefits and risks. However, in elective treatment it is not acceptable for the patient to receive no information about anaesthesia until their pre-operative visit from the anaesthetist: at such a late stage the patient will not be in a position genuinely to make a decision about whether or not to undergo anaesthesia. Patients should therefore either receive a general leaflet about anaesthesia in out-patients or have the opportunity to discuss anaesthesia in a pre- assessment clinic. The anaesthetist should ensure that the discussion with the patient and their consent is documented in the anaesthetic record, in the patient's notes or on the consent form. W here the clinician providing the care is personally responsible for anaesthesia (e.g. where local anaesthesia or sedation is being used), then he or she will also be responsible for ensuring that the patient has given consent to that form of anaesthesia.

In addition, where general anaesthesia or sedation is being provided as part of dental treatment, the General Dental Council currently holds dentists responsible for ensuring that the patient has all the necessary information. In such cases, the anaesthetist and dentist will therefore share that responsibility.

3.5 Emergencies

Clearly in emergencies, the two stages (discussion of options and confirmation that the patient wishes to go ahead) will follow straight on from each other, and it may often be appropriate to use the patient's notes to document any discussion and the patient's consent, rather than using a form. The urgency of the patient's situation may limit the quantity of information that they can be given but should not affect its quality.

3.6 Treatment of Children

The legal position concerning consent and refusal of treatment by those under the age of 18 is different from the position for adults. For the purposes of this guidance 'children' refers to people aged below 16 and 'young people' refers to people aged 16–17.

3.6.1 Young people aged 16–17

By virtue of section 8 of the Family Law Reform Act 1969, people aged
16 or 17 are presumed to be capable of consenting to their own medical treatment, and any ancillary procedures involved in that treatment, such as an anaesthetic. As for adults, consent will be valid only if it is given voluntarily by an appropriately informed young person capable of consenting to the particular intervention. However, unlike adults, the refusal of a competent person aged 16–17 may in certain circumstances be overridden by either a person with parental responsibility or a court (see paragraphs 14–18 below).

Section 8 of the Family Law Reform Act 1969 applies only to the young person's own treatment. It does not apply to an intervention that is not potentially of direct health benefit to the young person,

such as blood donation or non-therapeutic research on the causes of a disorder. However, a young person may be able to consent to such an intervention under the standard of Gillick competence, considered below (see paragraph 6 et seq.).

In order to establish whether a young person aged 16 or 17 has the requisite capacity to consent to the proposed intervention, the same criteria as for adults should be used. If a young person lacks capacity to consent because of an impairment of, or a disturbance in the functioning of, the mind or brain then the Mental Capacity Act 2005 will apply in the same way as it does to those who are 18 and over. If however they are unable to make the decision for some other reason, for example because they are overwhelmed by the implications of the decision, then the Act will not apply to them and the legality of any treatment should be assessed under common law principles. It may be unclear whether a young person lacks capacity within the meaning of the Act. In those circumstances, it would be prudent to seek a declaration from the court.

If the 16/17-year-old is capable of giving valid consent, then it is not legally necessary to obtain consent from a person with parental responsibility for the young person in addition to the consent of the young person. It is, however, good practice to involve the young person's family in the decision- making process – unless the young person specifically wishes to exclude them – if the young person consents to their information being shared.

3.6.2 Children under 16 – the concept of Gillick competence

In the case of Gillick, the court held that children who have sufficient understanding and intelligence to enable them to understand fully what is involved in a proposed intervention will also have the capacity to consent to that intervention. This is sometimes described as being 'Gillick competent'. A child of under 16 may be Gillick competent to consent to medical treatment, research, donation or any other activity that requires their consent.

The concept of Gillick competence is said to reflect a child's increasing development to maturity. The understanding required for different interventions will vary considerably. Thus a child under 16 may have the capacity to consent to some interventions but not to others. The child's capacity to consent should be assessed carefully in relation to each decision that needs to be made.

In some cases, for example because of a mental disorder, a child's mental state may fluctuate significantly, so that on some occasions the child appears Gillick competent in respect of a particular decision and on other occasions does not. In cases such as these, careful consideration should be given as to whether the child is truly Gillick competent at the time that they need to take a relevant decision.

If the child is Gillick competent and is able to give voluntary consent after receiving appropriate information, that consent will be valid and additional consent by a person with parental responsibility will not be required. It is, however, good practice to involve the child's family in the decision-making process, if the child consents to their information being shared.

3.6.2.1 The requirement of voluntariness

Although a child or young person may have the capacity to give consent, this is only valid if it is given voluntarily. This requirement must be considered carefully.

Children and young people may be subject to undue influence by their parent(s), other carers or a sexual partner (current or potential), and it is important to establish that the decision is that of the individual him or herself.

3.6.2.2 Child or young person with capacity refusing treatment

W here a young person of 16 or 17 who could consent to treatment in accordance with section 8 of the Family Law Reform Act 1969, or a child under 16 but Gillick competent, refuses treatment, it is possible that such a refusal could be overruled if it would in all probability lead to the death of the child/young person or to severe permanent injury.

A life-threatening emergency may arise when consultation with either a person with parental responsibility or the court is impossible, or the person with parental responsibility refuses consent despite such emergency treatment appearing to be in the best interests of the child. In such cases the courts have stated that doubt should be resolved in favour of the preservation of life, and it will be acceptable to undertake treatment to preserve life or prevent serious damage to health.

3.6.2.3 Child lacking capacity

W here a child under the age of 16 lacks capacity to consent (i.e. is not Gillick competent), consent can be given on their behalf by any one person with parental responsibility (if the matter is within the 'zone of parental control) or by the court. As is the case where patients are giving consent for themselves, those giving consent on behalf of child patients must have the capacity to consent to the intervention in question, be acting voluntarily and be appropriately informed. The power to consent must be exercised according to the 'welfare principle': that the child's 'welfare' or 'best interests' must be paramount. Even where a child lacks capacity to consent on their own behalf, it is good practice to involve the child as much as possible in the decision- making process.

The European Court of Human Rights judgment in a case where doctors treated a child contrary to his mother's wishes, without a court order (Glass v United Kingdom), made clear that the failure to refer such cases to the court is not only a breach of professional guidance but also potentially a breach of the European Convention on Human Rights. In situations where there is continuing disagreement or conflict between those with parental responsibility and doctors, and where the child is not competent to provide consent, the court should be involved to clarify whether a proposed treatment, or withholding of treatment, is in the child's best interests. Parental refusal can only be overridden in an emergency.

The Children Act 1989 sets out persons who may have parental responsibility. These include: the child's mother, the child's father, if he was married to the mother at the time of birth unmarried fathers, who can acquire parental responsibility in several different ways:

For children born before 1 December 2003, unmarried fathers will have parental responsibility if they: a) marry the mother of their child or obtain a parental

responsibility order from the court b) register a parental responsibility agreement with the court or by an application to court.

For children born after 1 December 2003, unmarried fathers will have parental responsibility if they: a) register the child's birth jointly with the mother at the time of birth, b) re-register the birth if they are the natural father, c) marry the mother of their child or obtain a parental responsibility

order from the court, d) register with the court for parental responsibility the child's legally appointed guardian, a person in whose favour the court has made a residence order concerning the child, a local authority designated in a care order in respect of the child.

Consent given by one person with parental responsibility is valid, even if another person with parental responsibility withholds consent. However, the courts have stated that a 'small group of important decisions' should not be taken by one person with parental responsibility against the wishes of another. W here persons with parental responsibility disagree as to whether these procedures are in the child's best interests, it is advisable to refer the decision to the courts. It is possible that major experimental treatment, where opinion is divided as to the benefits it may bring the child, might also fall into this category of important decisions, although such a case has not yet been considered in the English courts.

here there is doubt about whether a parent is acting in the interests of the child or young person, then the healthcare practitioner would be unwise to rely on the parent's consent, for example if a child alleges abuse and the parent supports psychiatric treatment for the child. The Government's guidance Working Together to Safeguard Children covers situations involving parental consent where abuse or neglect is suspected.

In order to consent on behalf of a child, the person with parental responsibility must themselves have capacity. W here the person with parental responsibility for a child is themself under 18, they will only be able to give valid consent for the child's treatment if they themselves are Gillick competent (see above) Whether or not they have capacity may vary, depending on the seriousness of the decision to be taken.

W here a child is a ward of court, no important step may be taken in the life of the child without the prior consent of the court. This is likely to include more significant medical interventions but not treatment for minor injuries or common diseases of childhood.

In an emergency, it is justifiable to treat a child who lacks capacity without the consent of a person with parental responsibility, if it is impossible to obtain consent in time and if the treatment is vital to the survival or health of the child.

3.7 Who is responsible for seeking consent?

The health professional carrying out the procedure is ultimately responsible for ensuring that the patient is genuinely consenting to what is being done: it is they who will be held responsible in law if this is challenged later.

W here oral or non-verbal consent is being sought at the point the procedure will be carried out, this will naturally be done by the health professional responsible.

However, team-work is a crucial part of the way the NHS operates, and where written consent is being sought it may be appropriate for other members of the team to participate in the process of seeking consent.

The Royal College of Surgeon's Guide to Good Practice, "Consent: Supported Decision-Making", says, "the surgeon discussing treatment with the patient should be suitably trained and qualified to provide the treatment in question and have sufficient knowledge of the associated risks and

complications, as well as any reasonable alternative treatments available for the patient's condition".

This is supplemented with the acknowledgment that "for minor investigative procedures" as opposed to treatment, it is reasonable for staff who have had specific training to carry out the consent discussion with the patient."

It will be noted that there is no requirement for the actual surgeon who is going to undertake the procedure to obtain the consent, but that the person must be, "an experienced member of the surgical team who has the time and skill to gain sufficient understanding of the patient's views and wishes".

It is said in addition that, "trainers will need to give particular consideration to how trainees can acquire the skills needed to comply with the new standards set out in this guidance and in law".

Guidance is simply that: it is guidance. It does not establish a standard of care, although it can be strong evidence of the appropriate standard. That is to say, it is not necessarily negligent to fail to comply with local or national or international guidance, but ordinarily this would require justification. Indeed, a departure may well need to be addressed as part of the consenting process.

Drawing the legal and regulatory framework together then, there is no general prohibition on delegating the process of obtaining consent. It seems possible to discern the following general principles:

- The person taking consent must be appropriately experienced.
- They must be suitably trained and qualified to provide the treatment in question.
- If we are not concerned with treatment, but only with a minor investigative procedure, they need not be qualified to undertake the investigation, so long as they have had proper training.
- They must have appropriate knowledge of the associated risks and complications.
- They must be able to apply the subjective test as per Montgomery, recognising the individual characteristics of the patient. Accordingly they must either take or have access to a detailed history.
- They must have knowledge of reasonable alternative treatments (and potentially different techniques of delivering the same treatment), which will involve a process of ongoing education and keeping abreast of developing literature and guidance, in the usual way.

3.8 Process for identifying staff who are not capable of performing the procedure but who are authorised to obtain consent

3.8.1 Medical Staff (SpR)

New medical staff at SpR level joining Liverpool Heart and Chest Hospital will be identified by the Consultant for that speciality they are joining as able to obtain consent for specific procedures. The record will identify who is to undergo training in order to take procedure specific consent.

SpR starters who have previously rotated to this organisation in the past, and who have been identified as able to take consent by the Consultant, having received procedure specific training

will be required to undertake refresher training, to be delivered by the Consultant for that speciality, either on a one to one basis, or as part of a training programme. It is the Consultants responsibility to ensure that medical staff under their supervision have completed record of competency forms prior to undertaking consent for a procedure on their behalf. Formal records of new starter SpR and rejoining SpR staff who are identified as not capable of performing the procedure but who are authorised to obtain consent will be kept by the Post Graduate Medical Education Department.

They will not undertake to obtain consent until they have received procedure specific training and have been found competent to undertake consent for that procedure. (Appendix H relates to consent for surgical procedures & Appendix J relates to consent for Cardiology Procedures for Chest Medicine).

They will be required to attend generic training on the consent process annually.

3.8.2 Clinical Nurse Practitioners

Clinical Nurse Practitioners (CNP) employed within Cardiology will be identified as able to obtain consent for specific procedures as agreed by the Consultant for that speciality. This will include Box Change, PCI and PPM insertion. Once they have received procedure specific training and been assessed and had the competency checklist signed off by the Consultant, they will be deemed able to obtain consent, but not able to perform the procedure.

The Team Leader for the Clinical Nurse Practitioners will keep an accurate record of the Clinical Nurse Practitioners who have been identified as able to take consent once they have received procedure specific training, but who are not able to perform the procedure.

They will be required to attend generic training on the consent process annually.

3.8.3 Cardiac Physiologists

Cardiac Physiologists employed within Cardiology will be identified as able to obtain consent for procedures known as tilt testing, as agreed by the Consultant for that speciality.

Once they have received procedure specific training and been assessed and had the competency checklist signed off by the Consultant, they will be deemed able to obtain consent and carry out the procedure.

The Team Leader for the Cardiac Physiologists will keep an accurate record of the Cardiac Physiologists who have been identified as able to take consent once they have received procedure specific training.

They will be required to attend generic training on the consent process annually.

3.8.4 Advanced Nurse Practitioners

Advanced Nurse Practitioners (ANP) employed within Cardiology will be identified as able to obtain consent for specific procedures as agreed by the Consultant for that speciality. This will include ACS transfers, Angiography and PCI. Once they have received procedure specific

training and been assessed and had the competency checklist signed off by the Consultant, they will be deemed able to obtain consent, but not able to perform the procedure.

They will be required to attend generic training on the consent process annually.

3.8.5 Specialist Nurses

Specialist Nurses employed within cardiology will be identified as able to obtain consent for specific procedures as agreed by the clinical lead for that specialty. Once they have received procedure specific training and been assessed and had the competency checklist signed off by the Consultant, they will be deemed able to obtain consent, but not able to perform the procedure.

They will be required to attend generic consent training on an annual basis.

Process for following up those who have obtained consent for a procedure without being authorised to do so

Staff who obtain consent for a procedure without the authority to do so, will be identified by means of auditing the consent process. The audit department will conduct an annual audit of consent. They will be referred to the Post Graduate tutor or team leader by the Education Officer.

A record will be kept on the staff members Personal Development Record. The Post Graduate Tutor will write to the staff member immediately advising them they must ensure they have received the appropriate training in order to take consent and that they have completed and sent back to the Education department the required competency assessment sheets. They will be advised that they cannot continue to take consent until they have completed the relevant training. Failure to do this will result in the staff member having requests for study leave and/or annual leave being refused until the forms are received.

3.9 GMC notification

Doctors will be reminded by the Education Officer on two occasions that they must submit completed consent competency forms. Failure to heed the reminders leads to the Post Graduate Tutor being informed, who will write to the Doctor concerned, informing them that continued failure to provide the evidence will lead to the GMC being informed. The GMC will be informed using the form available at quality@gmc- uk.org if there is repeated failure to provide evidence of the completed consent competency form.

3.10 Provision of Information

The provision of information is central to the consent process. Before patients can come to a decision about treatment, they need comprehensible information about their condition and about possible treatments/investigations and their risks and benefits (including the risks / benefits of doing nothing) as well as alternative treatments and those not offered at the Trust including those available outside the UK. They also need to know whether additional procedures are likely to be necessary as part of the procedure, for example a blood transfusion, or the removal of particular tissue. Once a decision to have a particular treatment / investigation has been made, patients need information about what will happen: where to go, how long they will be in hospital, how they will feel afterwards and so on.

A proper discussion of alternatives must take place and this has recently been considered by the Court in Bayley v George Eliot Hospital NHS Trust. The patient alleged her treating clinicians should have advised her of all treatment options, including those available to her outside of the UK. Specifically, it was alleged they had failed to advise her that her DVT could be treated by an ilio-femoral venous stent. The Judge determined that an alternative treatment option must be within the knowledge of a reasonably competent clinician; it must represent “accepted” practice; and must be an ‘appropriate treatment’ and not just a ‘possible treatment’.

Patients and those close to them will vary in how much information they want: from those who want as much detail as possible, including details of rare risks, to those who ask health professionals to make decisions for them. There will always be an element of clinical judgment in determining what information should be given. However, the presumption must be that the patient wishes to be well informed about the risks and benefits of the various options. W here the patient makes clear (verbally or non-verbally) that they do not wish to be given this level of information, this should be documented.

The following sources of patient information are available in this Trust:

A range of Patient information leaflets – available within each department - details available from Customer Services Team.
There is a flowchart available on the intranet which details the process for developing and/or updating patient information, in addition there is detailed guidance available within each directorate and for each writing group. All information will be approved through the Information for patients group following review by the lay reading group.
Information can be converted in to Braille on request; this should be done through the Customer Service Team.

The Patient Information policy holds more detail with regards to patient information and includes archiving arrangements of information given to patients

3.11 Montgomery and Informed Consent, and Other Relevant Case Law

The Montgomery versus Lanarkshire case of March 2015 was a landmark for informed consent in the UK. Nadine Montgomery, a woman with diabetes and of small stature, delivered her son vaginally; he experienced complications owing to shoulder dystocia, resulting in hypoxic insult with consequent cerebral palsy. Her obstetrician had not disclosed the increased risk of this complication in vaginal delivery, despite Montgomery asking if the baby’s size was a potential problem. Montgomery sued for negligence, arguing that, if she had known of the increased risk, she would have requested a caesarean section. The Supreme Court of the UK announced judgment in her favour in March 2015. The ruling overturned a previous decision by the House of Lords which had been law since at least the mid 1980s. It established that, rather than being a matter for clinical judgment to be assessed by professional medical opinion, a patient should be told whatever they want to know, not what the doctor thinks they should be told.

The Montgomery decision redefined the standard for informed consent and disclosure. Previously, the Bolam test in England was used to determine what should be disclosed. These tests ask whether a doctor’s conduct would be supported by a responsible body of clinicians. The Bolam test was affirmed in Sidaway v Bethlem Royal Hospital Governors and others, although the ruling was not unanimous, with judges placing different weight on the patient’s right to make informed treatment decisions versus the doctor’s professional judgment in disclosing information. The

Montgomery case firmly rejected the application of Bolam to consent, establishing a duty of care to warn of material risks. The key passages from the Montgomery judgment involve what a patient would consider to be material risk:

'The doctor is therefore under a duty to take reasonable care to ensure that the patient is aware of any material risks involved in any recommended treatment, and of any reasonable alternative or variant treatments'.

'The test of materiality is whether, in the circumstances of the particular case:
a reasonable person in the patient's position would be likely to attach significance to the risk,
or the doctor is or should reasonably be aware that the particular patient
would be likely to attach significance to it'.

Some other key points were:

- Whether a risk is material doesn't only depend on how frequently it occurs
- Your advisory role involves talking to the patient to make sure they understand the risks and benefits of their treatment, so that they can make an informed
- decision
- Simply providing the information or getting a signature on a consent form may not be enough to evidence proper consent, but can be helpful as part of the consent process

The Montgomery case clashes patient autonomy against medical paternalism. In reality, medical decision making involves a nuanced negotiation of information. Today's patients can expect a more active and informed role in treatment decisions, with a corresponding shift in emphasis on various values, including autonomy, in medical ethics.

Although Montgomery changed the legal position, the principle of involving patients in their treatment and sharing information with them about risks has been in place for some time. This is reflected in the GMC guidance, 'Consent: doctors and patients making decisions together' (2009). In particular, paragraph 28 from that guidance states that, 'the amount of information …… will depend on the individual patient and what they want or need to know.' To use the terminology of the Supreme Court, the assessment is "fact-sensitive, and sensitive also to the characteristics of the patient."

3.11.1 Therapeutic exception

In a situation where being given this information would be seriously detrimental to the patient's health, the Supreme Court ruled that it can be withheld. However, this is a limited exception and it is likely that it will only be applicable in very rare circumstances.

3.11.2 Other Relevant Case Law

There are some other cases which warrant brief mention by way of context:

In Spencer v Hillingdon Hospital NHS Trust, the Trust were held liable for failure, prior to the patient's discharge after a hernia operation under general anaesthetic, to warn him of the signs and symptoms of DVT or pulmonary embolism or of the risk that he might develop those conditions. There was some debate as to the likelihood of the risk eventuating, but it was

understood by the profession that it could do so, and such advice was suggested in NICE guidance.

In A v East Kent Hospitals, the complaint was of failure to advise a mother that her baby might be suffering from a very rare chromosomal abnormality. The Judge rejected the Claimant's case on the grounds that although there was a risk, it was theoretical, negligible or background risk of the order of 1 in 1000 and thus was not a material risk. The Judge held that Montgomery was not authority for the proposition that medical practitioners need to warn about risks which are theoretical and not material.

In Tasmin v Barts Health NHS Trust, the Judge reached a similar decision in respect of a 1 in 1000 risk saying that, wherever the borderline between materiality and non-materiality lay (as to which he made no finding), such a risk was too low to be material.

In Thefaut v Francis Johnson, the evidence established clearly (in the context of back surgery), that doing nothing is an option which ought to be considered, where there were reasonable prospects of improvement without surgery, as set against a risk of exacerbated problems following surgery. The judgment also highlighted that a simple signature on a consent form is not definitive evidence of an acceptance of risk and that, immediately prior to surgery is not the time or place to start explaining risks for the first time.

3.11.3 Summary

When seeking consent to treatment, the question of whether the information given to a patient is adequate is judged from the perspective of a reasonable person in the patient's position.
For the purpose of consent, the ruling from Montgomery replaces the previous tests founded in Bolam and refined in Sidaway.

Doctors have a duty to take reasonable care to ensure that patients are aware of 'material risks'.

3.12 Provision for patients whose first language is not English

This Trust is committed to ensuring that patients whose first language is not English receive the information they need and are able to communicate appropriately with healthcare staff. It is not appropriate to use children or another family member to interpret for family members who do not speak English. An interpreter must be arranged in this instance.

Interpreter service and language line details are available from the Customer Services Team. There is a list of staff able to communicate in a different language available from this department also.

3.12.1 Written consent

Consent is often wrongly equated with a patient's signature on a consent form. A signature on a form is evidence that the patient has given consent, but is not proof of valid consent. If a patient is rushed into signing a form, on the basis of too little information, the consent may not be valid, despite the signature. Similarly, if a patient has given valid verbal consent, the fact that they are physically unable to sign the form is no bar to treatment. Patients may, if they wish, withdraw consent after they have signed a form: the signature is evidence of the process of consent-giving, not a binding contract.

It is rarely a legal requirement to seek written consent, but it is good practice to do so if any of the following circumstances apply:

The treatment or procedure is complex, or involves significant risks (the term ‘risk’ is used throughout to refer to any adverse outcome, including those which some health professionals would describe as ‘side-effects’ or ‘complications’):

The procedure involves general / local anaesthesia or sedation

Providing clinical care is not the primary purpose of the procedure

There may be significant consequences for the patient’s employment, social or personal life

The treatment is part of a project or programme of research approved by this Trust.

Completed forms should be kept with the patient’s notes. Any changes to a form, made after the form has been signed by the patient, should be initialled and dated by both patient and health professional.

It will not usually be necessary to document a patient’s consent to routine and low-risk procedures, such as providing personal care or taking a blood sample. However, if you have any reason to believe that the consent may be disputed later or if the procedure is of particular concern to the patient (for example if they have declined, or become very distressed about, similar care in the past), it would be helpful to do so.

The Mental Health Act 1983, 2005, 2007 and the Human Fertilisation and Embryology Act 1990 require written consent in certain circumstances.

3.12.2 Responsibility of health professionals

It is a health professional’s own responsibility:

To ensure that when they require colleagues to seek consent on their behalf they are confident that the colleague is competent to do so; and
To work within their own competence and not to agree to perform tasks
which exceed that competence.

If you feel that you are being pressurised to seek consent when you do not feel competent to do so you can contact Deputy Director of Nursing, Risk Manager, or Medical Director.

3.13 Adults without capacity

The Mental Capacity Act 2005 came fully into force in October 2007 and applies in England and W ales to everyone who works in health and social care and is involved in the care, treatment or support of people over 16 years of age who may lack capacity to make decisions for themselves.

Under English law, no one is able to give consent to the examination or treatment of an adult who lacks the capacity to give consent for themselves, unless they have been authorised to do so under a Lasting Power of Attorney or they have the authority to make treatment decisions as a

court appointed deputy. Therefore, in most cases, parents, relatives or members of the healthcare team cannot consent on behalf of such an adult. However, the Mental Capacity Act sets out the circumstances in which it will be lawful to carry out such examinations or treatment.

In general, the refusal to an intervention made by a person when they had capacity cannot be overridden if the advance decision is valid and applicable to the situation.

The legal requirements in the Mental Capacity Act are underpinned by five statutory principles. One of these key principles is that any act done for, or any decision made on behalf of, a person who lacks capacity must be done, or made, in that person's best interests. This principle applies to health professionals as it does to anyone working with and caring for a person who lacks capacity. The Act also creates a new offence of ill treatment or wilful neglect of someone who lacks capacity by someone with responsibility for their care or with decision-making powers.

The Mental Capacity Act provides healthcare professionals with protection from civil and criminal legal liability for acts or decisions made in the best interests of the person who lacks capacity. The Act makes it clear that when determining what is in a person's best interests a healthcare professional must not make assumptions about someone's best interests merely on the basis of the person's age or appearance, condition or any aspect of their behaviour.

The Act requires that a healthcare professional must consider all the relevant circumstances relating to the decision in question. These are described as factors that the healthcare professional is aware of and which are reasonable to take into account.

In considering the relevant circumstances, the Act rules that the healthcare professionals must take the following steps:

- Consider whether the person is likely to regain capacity and if so whether the decision can wait.
- Involve the person as fully as possible in the decision that is being made
- on their behalf.
- As far as possible, consider:
- The person's past and present wishes and feelings (in particular if they have been written down)
- Any beliefs and values (e.g. religious, cultural or moral) that would be likely to influence the decision in question, and any other relevant factors, and the other factors that the person would be likely to consider if they were able to do so.

As far as possible, consult other people if it is appropriate to do so and take into account their views as to what would be in the best interests of the person lacking capacity, especially:

- anyone previously named by the person lacking capacity as someone to be consulted
- anyone engaging in caring for or interested in the person's welfare
- any attorney appointed under a Lasting Power of Attorney
- any deputy appointed by the Court of Protection to make decisions for the person

For decisions about serious medical treatment, where there is no one appropriate other than paid staff, healthcare professionals have to instruct an IMCA

If the decision concerns the provision or withdrawal of life-sustaining treatment, the person making the best interests decision must not be motivated by a desire to bring about the person's death.

The Mental Capacity Act (2005) Code of Practice makes it clear that the steps set out in the Act should form the starting point for considering all the relevant circumstances of each case, and often other factors will be important.

Healthcare professionals should demonstrate in their record-keeping that the decision has been based on all available evidence and has taken into account any conflicting views. What is in a person's best interests may well change over time. This means that even where similar actions need to be taken repeatedly in connection with the person's care or treatment, the person's best interests should be reviewed regularly.

In cases of serious doubt or dispute about an individual's mental capacity or best interests, an application can be made to the Court of Protection for a ruling. The duty officer of the Official Solicitor can advise on the appropriate procedure if necessary.

3.13.1 Duration of lack of capacity

The provisions of the Mental Capacity Act apply to acts or decisions made on behalf of an adult who lacks capacity – whether the lack of capacity is likely to be temporary or permanent. It is possible for capacity to fluctuate. In such cases, it is good practice to establish, while the person has capacity, their views about any clinical intervention that may be necessary during a period of anticipated incapacity, and to record these views. The person may wish to make an advance decision to refuse treatment or a statement of their preferences and wishes. If the person does not make a relevant advance decision, decisions about that person's treatment if they lack capacity must be made in accordance with the Mental Capacity Act. This would include considering whether the person is likely to regain capacity and, if so, whether the decision can wait, as well as the statutory principle that all practical steps must be taken to enable the person to make their own decision.

3.13.2 Statements of preferences and wishes

A healthcare professional must take all statements of a person's preferences and wishes into consideration as part of a best interest's assessment. Written statements which request specific treatments made by a person before losing capacity should be given the same consideration as those made by people who currently have capacity to make treatment decisions.

However, a healthcare professional would not have to follow a written request if they thought that the specific treatment would be clinically unnecessary or not appropriate for the person's condition, and therefore not in the person's best interests. If the decision is different to a written statement, a healthcare professional should keep a record of this and be prepared to justify the decision if challenged. There is an important legal distinction between a written statement expressing treatment preferences, which a healthcare professional must take into account when making a best interests decision, and a valid and applicable advance decision to refuse treatment, which healthcare professionals must follow. Healthcare professionals cannot ignore a written statement that is a valid and applicable advance decision to refuse treatment.

3.13.3 Lasting Power of attorney

The Mental Capacity Act enables a person aged 18 or o v e r to appoint an attorney to look after their health and welfare decisions if they should lack the capacity to make such decisions in the

future. Under a personal welfare LPA, the attorney – if they have the authority to do so – can make decisions that are as valid as those made by the person themselves. The LPA must be made in the form, and meet the criteria, set out in the regulations, and it must be registered with the Office of the Public Guardian before it can be used.

The LPA may specify limits to the attorney's authority, and the LPA must specify whether or not the attorney has the authority to make decisions about life- sustaining treatment. Healthcare practitioners directly involved in the care or treatment of a person who lacks capacity should not agree to act as that person's attorney other than in exceptional circumstances (for example if they are the only close relative of the person). If the person lacks capacity and has created a personal welfare LPA, the attorney will have the authority to make decisions and consent to or refuse treatment as set out in the LPA. Healthcare practitioners should read the LPA if it is available, in order to understand the extent of the attorney's power.

3.13.4 Court appointed deputies

If a person lacks capacity to make a decision relating to their personal welfare, then the Court of Protection can make an order making a decision on their behalf. Alternatively, the Court of Protection can appoint a deputy to make decisions on behalf of the person who lacks capacity. The Mental Capacity Act makes it clear that in such situations it is preferable for the Court of Protection to make the decision if at all possible, and that if a deputy is appointed, then their powers should be limited in scope to what is absolutely necessary.

The court must ensure that any deputy appointed has the necessary skills and abilities and is prepared to take on the duty and responsibility of the role. Both the court and any deputy must follow the statutory principles of the Act and make decisions in the person's best interests.

Deputies for personal welfare decisions will only be required in the most difficult cases, where important and necessary actions cannot be carried out without the

Court's authority or where there is no other way of settling the matter in the best interests of the person who lacks capacity. For example, a deputy could be appointed to make on-going decisions, having consulted all relevant parties. This could be useful where there is a history of family disputes.

If a deputy has been appointed to make treatment decisions on behalf of a person who lacks capacity, then it is the deputy rather t h a n the healthcare professional that makes the treatment decision. A deputy cannot go against a decision of an attorney under an LPA made before the person lacks capacity. Deputies must follow the Mental Capacity Act's statutory principles and must make decisions in the person's best interests. A deputy cannot refuse consent to the provision of life-sustaining treatment

3.14.4 Independent mental capacity advocates

The Mental Capacity Act has, since April 2007 in England and since October 2007 in W ales, introduced a duty on NHS bodies to instruct an IMCA in serious medical treatment decisions when a person who lacks capacity to make a decision has no one who can speak for them, other than paid staff. In matters that meet the definition of serious medical treatment, IMCAs are only able to represent and support people whose treatment is arranged by the NHS. They have the right to information about an individual and can see relevant healthcare records.

The duties of an IMCA are to:

- support the person who lacks capacity and represent their views and interests to the decision-maker
- obtain and evaluate information, both through interviewing the person and through examining relevant records and documents
- obtain the views of professionals providing treatment for the person who lacks capacity
- identify alternative courses of action
- obtain a further medical opinion, if required, and
- prepare a report (that the decision-maker must consider).

IMCAs are not decision-makers for the person who lacks capacity. They are there to support and represent that person and to ensure that decision-making for people who lack capacity is done appropriately and in accordance with the Mental Capacity Act. More information is given at www.dh.gov.uk/imca and in chapter 10 of the Mental Capacity Act (2005) Code of Practice.

3.14.4.1 Consent forms

Where treatment is provided to a person who lacks capacity following a best interests decision, any consent form should not be signed by someone else unless they have a personal welfare LPA that authorises them to make the decision in question, or they are a court appointed deputy with similar authority. It is good practice to note either in the records or on a 'patient unable to consent' form why the treatment was decided to be in the patient's best interests.

3.14.4.2 Referral to court

The Mental Capacity Act established the Court of Protection to deal with decision-making for adults (and children in a few cases) who may lack the capacity to make specific decisions for themselves. The Court of Protection deals with serious decisions affecting personal welfare matters, including healthcare, which were previously dealt with by the High Court.
In cases of serious dispute, where there is no other way of finding a solution or when the authority of the court is needed in order to make a particular decision or take a particular action, the court can be asked to make a decision.

The courts have identified certain circumstances when referral should be made to them for a ruling on lawfulness before a procedure is undertaken. These are:

decisions about the proposed withholding or withdrawal of ANH from patients in a permanent vegetative state

cases involving organ, bone marrow or peripheral blood stem cell donation by an adult who lacks the capacity to consent

all other cases where there is a doubt or dispute about whether a particular treatment will be in a person's best interests.

Other cases likely to be referred to the court include those involving ethical dilemmas in untested areas (such as innovative treatments for variant CJD44), or where there are otherwise irresolvable conflicts between healthcare staff, or between staff and family members.

3.15 Refusal of Treatment

If the process of seeking consent is to be a meaningful one, refusal must be one of the patient's options. A competent adult patient is entitled to refuse any treatment, except in circumstances governed by the Mental Health Act 1983. The situation for children is more c o m p l e x : see the Department of Health's Seeking consent : working with children for more detail. The following paragraphs apply primarily to adults.

If, after discussion of possible treatment options, a patient refuses all treatment, this fact should be clearly documented in their notes. If the patient has already signed a consent form, but then changes their mind, you (and where possible the patient) should note this on the form.

W here a patient has refused a particular intervention, you must ensure that you continue to provide any other appropriate care to which they have consented. You should also ensure that the patient realises they are free to change their mind and accept treatment if they later wish to do so. W here delay may affect their treatment choices, they should be advised accordingly.

If a patient consents to a particular procedure but refuses certain aspects of the intervention, you must explain to the patient the possible consequences of their partial refusal. If you genuinely believe that the procedure cannot be safely carried out under the patient's stipulated conditions, you are not obliged to perform it. You must, however, continue to provide any other appropriate care. W here another health professional believes that the treatment can be safely carried out under the conditions specified by the patient, you must on request be prepared to transfer the patient's care to that health professional.

3.16 Tissue

The legal position regarding the use of human tissue (including blood samples and other bodily fluids provided for testing) raises some difficult issues and is currently under review.
Such tissue can be very valuable in education and research, and its use may lead to developments in medical l knowledge and hence improvements in healthcare for all. At present, this Trust requires that patients should be given the opportunity to refuse permission for tissue taken from them during surgery or other procedure to be used for education or research purposes. All patients who are potential participants in our ongoing research program undergo an informed consent process specific to the research in question, supported by a patient information leaflet. Tissue will only be removed from patients giving this consent; a copy of their consent form is filed in the case notes.

Explicit consent is not necessary for public health surveillance using the unlinked anonymous method, but a well-publicised opt-out policy must apply. The provision of information during informed consent should include detail of any potential for retained tissue to be utilised for public health surveillance.

Pending the outcome of the review of the law governing the use of human organs and tissue, the Department of Health believes that tissue samples may be used for quality assurance purposes without requiring specific patient consent provided there is an active policy of informing patients of such use. This is essential to ensure the high quality of service which all patients have the right to expect. Wherever possible, samples of tissue used in this way should be anonymised or pseudonymised. The provision of information during informed consent should include detail of any potential for retained tissue to be utilised for quality assurance.

3.17 Clinical photography and conventional or digital video recordings

Photographic and video recordings made for clinical purposes form part of a patient's record. Although c o n s e n t to certain recordings, such as X -rays, is implicit in the patient's consent to the procedure, health professionals should always ensure that they make clear in advance if any photographic or video recording will result from that procedure.

Photographic and video recordings which are made for treating or assessing a patient must not be used for any purpose other than the patient's care or the audit of that care, without the express consent of the patient or a person with parental responsibility for the patient. The one exception to this principle is set out in paragraph 3 below. If you wish to use such a recording for education, publication or research purposes, you must seek consent in writing, ensuring that the person giving consent is fully aware of the possible uses of the material. In particular, the person must be made aware that you may not be able to control future use of the material once it has been placed in the public domain. If a child is not willing for a recording to be used, you must not use it, even if a person with parental responsibility consents.

Photographic and video recordings, made for treating or assessing a patient and from which there is no possibility that the patient might be recognised, may be used within the clinical setting for education or research purposes without express consent from the patient, as long as this policy is well publicised. However, express consent must be sought for any form of publication.

If you wish to make a photographic or video recording of a patient specifically for education, publication or research purposes, you must first seek their written consent (or where appropriate that of a person with parental responsibility) to make the recording, and then seek their consent to use it.

Patients must know that they are free to stop the recording at any time and that they are entitled to view it if they wish, before deciding whether to give consent to its use. If the patient decides that they are not happy for any recording to be used, it must be destroyed. As with recordings made with therapeutic intent, patients must receive full information on the possible future uses of the recording, including the fact that it may not be possible to withdraw it once it is in the public domain.

The situation may sometimes arise where you wish to make a recording specifically for education, publication or research purposes, but the patient is temporarily unable to give or withhold consent because, for example, they are unconscious. In such cases, you may make such a recording, but you must seek consent as soon as the patient regains capacity. You must not use the recording until you have received consent for its use, and if the patient does not consent to any form of use, the recording must be destroyed.

If the patient is likely to be permanently unable to give or withhold consent for a recording to be made, you should seek the agreement of some-one close to the patient. You must not make any use of the recording which might be against the interests of the patient. You should also not make, or use, any such recording if the purpose of the recording could equally well be met by recording patients who are able to give or withhold consent

3.18 Training

3.18.1 Generic consent training within the Liverpool Heart and Chest Hospital

It is a requirement for all Consultants, SpR, Cardiac Physiologists, Advanced Nurse Practitioners, specialist nurses (who take consent) and Clinical Nurse Practitioners to attend generic consent training as part of their Mandatory Training programme. This training covers any changes to legislation and any necessary changes that arise from the Trusts consent audits.

Attendance records will be maintained by the Education Department Non-attendance at Mandatory training will be reported to the Medical Director for actioning.

Process for the delivery of procedure specific training on consent, for staff to whom the consent process has been delegated and who are not capable of performing the procedure

Specific training for individual speciality on Consent within the Liverpool Heart and Chest Hospital is provided by a Consultant for that speciality. The professional groups identified below have been identified to obtain consent and who are not capable of performing the procedure can only do this after they have attended procedure specific training in their specialties.

SpR's will receive procedure specific training for Cardiology, Chest Medicine, Cardiac Surgery and Thoracic Surgery for those procedures listed on the competency forms.

Nurse practitioners receive procedure specific training for Cardiology for those procedures listed on the competency forms.

Advanced Nurse Practitioners and Cardiology Specialist nurses receive procedure specific training for cardiology for those procedures listed on the competency forms.

Procedure specific training will be conducted on a one to one session with the providing consultant.

When the training has been completed, the consultant will sign a Record of Competency to Obtain Consent to confirm that the trainee has been assessed as competent to obtain consent for explicit procedures.

For medical staff, competency checklists must be returned to the Education Department within two weeks of induction, where the staff will keep a centralised record of all SpR / Clinical Fellow / Staff Grade who have been delegated the responsibility to obtain consent on behalf of a consultant.

The Audit department perform an annual audit of health records; on occasions when SpR / Clinical Fellows / Staff Grades has taken consent, their name will be compared to the Education Dept. training records to ascertain whether or not a Record of Competency to Obtain Consent form for procedure specific consent has been completed prior to them obtaining consent from a patient.

The specific procedures for which staff may obtain consent are listed for each specialty in the following Appendices:

- Appendix H - Record of Competency to Obtain Consent for Cardiothoracic Surgical Procedures.

- Appendix J - Record of Competency to Obtain Consent for Cardiology and Chest Medicine

Procedures.

- Appendix K – example of Key Clinical Skills and Competencies for Clinical Nurse Practitioners (CNP's) and Advanced Nurse Practitioners (ANP's) to gain informed consent for Percutaneous Coronary Intervention (PCI).

- Appendix L – example of Key Clinical Skills and Competencies for Clinical Nurse Practitioners (CNP's) to gain informed consent for Permanent Pace Makers (PPM) Insertion & / PPM Generator Replacement (Box Change)

- Appendix M – Record of competency to obtain consent for Tilt Testing by Cardiac Physiologists

This section of the policy is subject to regular audit, and findings will be disseminated to the Medical Director and all Associate Medical Directors for their action.

3.19 Infections associated with heater cooler units used in cardio- pulmonary bypass and ECMO

Evidence to date indicates that heater cooler units used in cardiopulmonary bypass and extracorporeal membrane oxygenation (ECMO) can generate potentially infectious aerosols containing a range of bacteria including Mycobacterium chimaera. Public Health England (PHE) has mandated that patients are informed of the specific risk associated with these devices when they are consented for cardiac surgery (PHE publications gateway number: 2016541).

The risk to patients is estimated as:

- Cardiac valve repair/replacement – 1 in 5000
- CABG – 1 in 100,000
- Congenital heart disease – no cases associated with these procedures in the absence of heart valve surgery have been identified in the UK suggesting a very low risk of M. chimaera infection.
- There is a rising incidence rate from <0.2 before 2011 to 2 in 2014 per 10,000 person years of post-operative follow-up (assuming 5 years at risk after surgery). However, only one case operated on in 2015 at a national level has been diagnosed, and no cases have been diagnosed since the introduction of the enhanced cleaning and disinfection regime. These patients may still develop symptoms at a later date, but this may provide an early indication that the risk has already been reduced.

To reflect guidance from PHE, the consent forms for CABG and valvular surgery, as well as the general cardiac surgery consent form and the Cardiac Surgery information booklet for patients and families, have been updated to reflect this. The latter makes patients aware of the symptoms associated with this infection and that this can occur many years after surgery.

4. Policy Implementation Plan

5. Monitoring of Compliance

Compliance with the requirements of this policy will be monitored by means of an annual audit which is conducted by the Clinical Audit Department. Monitoring reports will be produced by the Education Department for the training element and the Complaints Manager for the Information elements of the policy. W here the report identifies deficiencies, the authors of the reports will produce an action plan to address these. The monitoring report and the action plan will be presented to the Clinical Quality Committee (training) and the Patient and Family Experience Committee (Information) who will be responsible for reviewing the action plan on at least a quarterly basis until the actions are complete.

6. References

7. Appendices

APPENDIX A

12 key points on consent: the law in England

When do health professionals need consent from patients?

1. Before you examine, treat or care for competent adult patients you must obtain their consent.

2. Adults are always assumed to be competent unless demonstrated otherwise. If you have doubts about their competence, the question to ask is: “can this patient understand and weigh up the information needed to make this decision?” Unexpected decisions do not prove the patient is incompetent but may indicate a need for further information or explanation.

3. Patients may be competent to make some health care decisions, even if they are not competent to make others.

4. Giving and obtaining consent is usually a process, not a one-off event. Patients can change their minds and withdraw consent at any time. If there is any doubt, you should always check that the patient still consents to your caring for or treating them.

   Can children give consent for themselves?

5. Before examining, treating or caring for a child, you must also seek consent.

   Young people aged 16 and 17 are presumed to have the competence to give consent for themselves. Younger children who understand fully what is involved in the proposed procedure can also give consent (although their parents will ideally be involved). In other cases, someone with parental responsibility must give consent on the child’s behalf, unless they cannot be reached in an emergency. If a competent child consents to treatment, a parent cannot override that consent. Legally, a parent can consent if a competent child refuses, but it is likely that taking such a serious step will be rare.

   Who is the right person to seek consent?

6. It is always best for the person actually treating the patient to seek the patient’s consent. However, you may seek consent on behalf of colleagues if you are capable of performing the procedure in question, or if you have been specially trained to seek consent for that procedure.

   What information should be provided?

7. Patients need sufficient information before they can decide whether to give their consent: for example information about the benefits and risks of the proposed treatment, and alternative treatments. If the patient is not offered as much information as they reasonably need to make their decision, and in a form they can understand, their consent may not be valid.

8. Consent must be given voluntarily: not u n d e r any form of duress or undue influence from health professionals, family or friends.

Does it matter how the patient gives consent?

9. No: consent can be written, oral or non-verbal. A signature on a consent form does not itself prove the consent is valid – the point of the form is to record the patient's decision, and also increasingly the discussions that have taken place. Your Trust organisation may have a policy setting out when you need to obtain written consent.

Refusal of treatment

10. Competent adult patients are entitled to refuse treatment, even when it would clearly benefit their health. The only exception to this rule is where the treatment is for a mental disorder and the patient is detained under the Mental Health Act 1983. A competent pregnant woman may refuse any treatment, even if this would be detrimental to the fetus.

Adults who are not competent to give consent

11. No-one can give consent on behalf of an incompetent adult. However, you may still treat such a patient if the treatment would be in their best interests. 'Best interests' go wider than best medical interests, to include factors such as the wishes and beliefs of the patient when competent, their current wishes, their general well-being and their spiritual and religious welfare. People close to the patient may be able to give you information on some of these factors. Where the patient has never been competent, relatives, carers and friends may be best placed to advise on the patient's needs and preferences.

12. If an incompetent patient has clearly indicated in the past, while competent, that they w o u l d refuse treatment in certain circumstances (an 'advance refusal'), and those circumstances arise, you must abide by that refusal.

This summary cannot cover all situations. For more detail, consult the Reference guide to consent for examination or treatment, available from www.doh.gov.uk/consent.

APPENDIX B

Current forms in use in this organisation Form 1 for adults or competent children;

A. Consent form Patient agreement to investigation or treatment
B. Consent form for Diagnostic Cardiac Catheterisation Patient agreement to investigation or treatment
C. Consent form for Percutaneous Coronary Intervention Patient agreement to investigation or treatment
D. Consent form for Coronary Artery Bypass Grafts Patient agreement to investigation or treatment
E. Consent Form for Valve Surgery Patient agreement to investigation or treatment
F. Consent Form for Cardiac Surgery Patient agreement to investigation or treatment
G. Consent Form for VATS Pleurectomy / Blebectomy Patient agreement to investigation or treatment
H. Consent Form for Bronchoscopy Lung Resection for cancer or suspected cancer Patient agreement to investigation or treatment
I. Consent Form for Bronchoscopy,+/- biopsy Mediastinoscopy,+/- biopsy Patient agreement to investigation or treatment

J. Consent form for Bronchoscopy VATS Thoracosocopy +/- biopsy Patient agreement to investigation or treatment
K. Consent form for Rigid bronchoscopy,+/- biopsy Patient agreement to investigation or treatment
L. Consent form for Oesophagoscopy,+/- dilation,+/- biopsy Patient agreement to investigation or treatment
M. Consent form for Bronchoscopy Oesophagoscopy Oesophageal resection Patient agreement to investigation or treatment
N. Consent form for VATS Sympathectomy Patient agreement to investigation or treatment

Form 2 Consent form for parental consent for a child or young person Parental agreement to investigation or treatment for a child or young person seldom used at Liverpool Heart and Chest Hospital please print from intranet under clinical policies consent.

Form 3 Consent form for cases where it is envisaged that the patient will remain alert throughout the procedure and no anaesthetist will be involved in their care not in use at Liverpool Heart and Chest Hospital please use Form 1.

Form 4 Consent form for adults who are unable to consent to investigation or treatment.

APPENDIX C

Useful contact details Medical Director Clinical Risk Manager

Deputy Director of Nursing
Patient Support Services and Complaints manager Medical Staffing and Education Manager

Ext 1706
Ext. 1653
Ext. 1631
Ext. 1257 Ext.1211

APPENDIX D

How to seek a Court Declaration

Please contact the Legal Services Manager Contact Trust legal advisors
Hill Dickinson
Pearl assurance house 2 Derby Square Liverpool
L2 9XL

Tel 0151 236 5400

APPENDIX E

Trust Specific items of policy and procedures undertaken requiring written consent Consent to ‘Do not Attempt Cardiopulmonary Resuscitation (DNACPR) Decisions’

Written guidance and support for clinicians
The General Medical Council (GMC) published wide-ranging guidance, Treatment and care towards the end of life: good practice in decision-making, in 2010
In 2001 the Resuscitation Council (UK) joined with the British Medical Association (BMA) and The Royal College of Nursing (RCN) to publish a joint statement on CPR decision-making.
The joint statement identified key ethical and legal issues that should inform all CPR decisions.
The statement provided general principles that allow local CPR policies to be tailored to local circumstances.
Six years later, in 2007, the three organisations published a revised statement.
This is called Decisions relating to cardiopulmonary resuscitation: A joint statement from the British Medical Association, the Resuscitation Council (UK) and the Royal College of Nursing.

The 2007 Joint Statement outlined ten main messages:-

1. Decisions about CPR must be made on the basis of an individual assessment of each patient's case.
2. It is not necessary to initiate discussion about CPR with a patient if there is no reason to believe that the patient is likely to suffer a cardiorespiratory arrest.
3. W here no explicit decision has been made in advance there should be an initial presumption in favour of CPR.
4. If CPR would not re-start the heart and breathing, it should not be attempted.
5. Advance care planning, including making decisions about CPR, is an important part of good clinical care for those at risk of cardiopulmonary arrest.
6. Communication and the provision of information are essential parts of good quality care.
7. W here the expected benefit of CPR may be outweighed by the burdens, the patient's informed views are of paramount importance. If the patient lacks capacity, those close to the patient should be involved in discussions to explore the patient's wishes, preferences, beliefs and values.
8. If a patient with capacity refuses CPR, or a patient lacking capacity has a valid and applicable advance decision refusing CPR, this should be respected.
9. A Do Not Attempt Cardiopulmonary Resuscitation DNACPR decision does not override clinical judgment in the unlikely event of a reversible cause of the patient's respiratory or cardiac arrest that does not match the circumstances envisaged.
10. DNACPR decisions apply only to CPR and not to any other aspects of treatment.

Overall responsibility for DNAR decisions rests with the consultant in charge of the patient's care

Please refer to the Trust's Cardiopulmonary Resuscitation Policy and Procedure Document on documenting and communicating a DNACPR decision.

Families and Post Mortems - A Code of Practice can be downloaded from the web site below.

Consent to Hospital Post Mortem examination on an adult.lnk
Relevant information and consent forms can be obtained from patient services.

Consent to Clinical Audit or Research Programmes
In general, clinical audit processes requiring access to clinical information, including case notes, may be carried out within the Trust without explicit consent provided that the Trust staff operate within a robust Confidentiality Code of Practice. The Data Protection Act should, however, always

be borne in mind, in that “information cannot be used for any other purpose than that for which it was intended" unless consent is obtained.

Written consent is required from the patients taking part in research projects.
The nature and purpose and what is known about the effects of any procedure(s) involved must be explained fully to the patient. The fact that the patient is participating in the project and the information that has been given to them must be noted in the case notes. All research must meet the requirements of the Local Research and Ethics Committee.

Consent to Involvement of Students
Patients should be asked if they object to being observed or treated by students. It should be clearly stated that all patients have the right to refuse without detriment to the care that they receive. It is good practice to include this information in patient information leaflets, appointment cards, etc. and on posters in waiting and ward areas.

Patients must also know the identity and status of the student(s) who are carrying out the assessments or treatment. If a student is required to see a patient on an unsupervised one to one basis, he/she must introduce him/herself and first gain the permission of the patient to the consultation.

APPENDIX F

Assessment of mental capacity-guidance notes
(Guidance must be read and understood before making assessment)

Core Principles
The Mental Capacity Act applies in England and W ales to everyone who works in health and social care and is involved in care.

- A person is assumed to have capacity. A lack of capacity has to be clearly demonstrated.
- No one should be treated as unable to make a decision unless all practicable (reasonable) steps to help them have been exhausted and shown not to work.
- A person can make an unwise decision. This does not necessarily mean they lack capacity.
- If it is decided a person lacks capacity then any decisions taken on their behalf must be in their best interests.
- Any decision taken on the behalf of a person who lacks capacity must taken into account their rights and freedom of action. Any decision should show that the least
- restrictive option or intervention is achieved.

Who is a relevant advocate?
As far as possible you must consult other people if it is appropriate to do so and take into account their views as to what would be in the best interests of the person lacking capacity, especially:

- anyone previously named by the person lacking capacity as someone to be consulted
- e.g. in an advance statement
- carers, close relatives or close friends or anyone else interested in the person’s welfare
- any attorney appointed under a Lasting Power of Attorney
- someone with the person’s Enduring Power of Attorney (financial matters)
- any deputy appointed by the Court of Protection to make decisions for the person.

For decisions about serious medical treatment, significant financial decisions or certain changes of accommodation and where there is no one who fits into any of the above categories, you may need to instruct an Independent Mental Capacity Advocate (IMCA).

Best Interests - the 7 Statutory Checklist Points:

- Don't make assumptions about a person's best interests.
- All relevant circumstances must be considered.
- Is the person likely to regain capacity, if so, can the decision wait?
- Involve the person as fully as possible.
- Decisions concerning the provision or withdrawal of life sustaining treatment must not be motivated by a desire to bring about a persons death.
- Consider the persons past and present wishes, their feelings together with any
- relevant beliefs or values. These may be written in an advance decision (refusal of treatment) and / or an advance statement (advance care planning) or a Lasting Power of Attorney.

You must consult other people if appropriate and take account of views, especially anyone previously named by the person as someone to be consulted. (Carers, close relatives or close friends or anyone else interested in the persons welfare); any attorney appointed under a Lasting Power of Attorney and any deputy appointed by the Court of Protection to make decisions for the person.

The "Decision Maker" weighs up all the information in order to determine what decision is in the person's best interests. Clear record keeping of the above is crucial. If in doubt contact Legal Services Department or the Risk and Clinical Governance Manager.

Can the decision be delayed because the person is likely to regain capacity in the near future? Careful consideration needs to be given to whether a person is likely to regain capacity with the time limits required by a decision. For example, is the person's understanding better at different times of the day or in particular contexts? Are they able to make decisions when they are in a comfortable environment, perhaps with loved ones in attendance? Consider the effects of medication over the course of the day.

Independent Mental Capacity Advocate (IMCA)

An IMCA is a specific type of advocate that will only have to be involved if there are no family or friends who can be consulted. An IMCA will not be the decision-maker, but you will have a duty to take into account the information given by the IMCA.

An IMCA will only be involved if:

- the decision is about serious medical treatment provided by the NHS
- it is proposed that the person be moved into long-term care of more than 28 days in a hospital or 8 weeks in a care home
- a long-term move (8 weeks or more) to different accommodation is being considered,
- for example, to a different hospital or care home.

Lasting Power of Attorney (LPA)

In October 2007 the Mental Capacity Act introduces Lasting Power of Attorney (LPA) which will allow people over the age of 18 to formally appoint someone to look after their health, welfare and/or financial decisions, if at some time in the future they lack the capacity to make these

decisions for themselves. The person appointed will be known as an attorney. The LPA will give the attorney authority to make decisions on behalf of the person and the attorney will have a duty to act or make decisions in the best interests of the person

- A personal welfare LPA is for decisions about both health and personal welfare
- A property and affairs LPA is for decision about financial matters

The attorney will be the decision-maker on all matters relating to the person's care and treatment. Unless the LPA specifies limits to the attorney's authority the attorney will have the authority to make personal welfare decisions and refuse treatment (except life-sustaining treatment unless the LPA specifies this) on the person's behalf. If there is a dispute that cannot be resolved, e.g. between the attorney and a doctor, it may have to be referred to the Court of Protection who may appoint a deputy to have ongoing authority to make decisions

It is important to read the LPA if it is available to understand the extent of the attorney's power. In order to be valid, the Lasting Power of Attorney must be in the prescribed format (contact Risk Management Dept. for sample of form). It must carry an official stamp and be registered with the Office of the Public Guardian. If in doubt as to the validity of the Lasting Power of Attorney, please contact 0300 456 0300 during office hours.

Deputy appointed by Court of Protection
A deputy appointed by the Court of Protection makes ongoing decisions about a person who lacks capacity. The Court of Protection will have defined the remit of their powers.

General Advocate
A General Advocate is a person from an Independent Advocacy Project or Service who listens to service users and gives them support to express their views. General Advocates can help service users in a range of ways for example, by ensuring they have access to information to make choices; by attending meetings to support service users and to ensure they are listened to; discovering what service the person's choices are.

Decision-Maker
The Decision-Maker is the person who is deciding whether to take action in connection with the care or treatment of an adult who lacks capacity or who is contemplating making a decision on their behalf:

- Where the decision involves medical treatment – the doctor proposing the treatment is the decision maker.
- W here nursing care is provided. The nurse is the decision-maker.
- For most day-to-day actions or decisions, the decision-maker will be the person most directly involved with the person at the time.

Outside hospital, the decision maker is likely to be care workers, family members, concerning day to day actions.
If there is a dispute then it should be clearly identified. If there is a dispute then the following things can assist the decision maker:

- Involve an advocate who is independent of all parties involved.
- Get a second opinion.
- Hold a formal or informal case conference.
- Go to mediation.
- Consider and discuss with your line manager and an application can be made to the Court

of Protection for a ruling.

ASSESSMENT OF CAPACITY AND BEST INTERESTS: RECORDING GUIDANCE
In working towards demonstrating compliance with the provisions of the Mental Capacity Act and yet keeping bureaucracy Liverpool Heart and Chest Hospital proposes two levels of recording by staff:

1. A capacity and best interest form required to be completed only in situations of specific life changing decisions regarding a client for whom capacity is an issue.

2. In relation to more general care, for all staff to start recording assessments of capacity and best interest decisions in regard to their own professional intervention within the recording system they currently use i.e. at initial assessment and reviews.

WHEN SHOULD THE FORM BE FILLED IN?
The Assessment of Capacity and Best Interest form should be filled in for persons without capacity, or for whom capacity for a decision or course of care or treatment is in doubt who are confronted with life changing decisions/events and specifically for persons without capacity where:

- There is conflict with the family.
- There are adult or public protection issues.
- There is an accommodation change e.g. to long term care, hospital admission, respite care, Change of tenancy.
- Any case conference convened around a serious issue.

SPECIFICALLY WHEN SHOULD HOSPITAL STAFF COMPLETE THE FORM?

- Where a patients admission is “informal” (i.e. the person is not detained under the Mental Health Act 1983) and there is an issue around a persons capacity. This area is important given that from 1st October 2007 Best Interest actions under common law no longer applies so that actions such as physical care intervention by nurses, medication giving etc. will need to be justified against and consistent with the Mental Capacity Act.
- Where there are restriction of liberty issues in relation to a person with capacity issues
- e.g. high level observations.

Where a patient is in hospital and there is conflict with family, adult protection issues or case conference convened in regard to a serious issue (i.e. as above).

Unless there are major changes in capacity or proposed interventions only one form should be completed per admission (with minor changes being recorded in routine clinical notes).

WHO SHOULD FILL IN THE ASSESSMENT FORM?
Many of these assessments will clearly be multidisciplinary given that they refer to life changing decisions / events where typically a number of professionals will be involved. The final responsibility of coordinating a capacity or Best Interest assessment will rest with the “Decision Maker”. The Decision Maker will be the main professional involved around the proposed decision / care and treatment.

WHAT GRADE OF STAFF SHOULD COMPLETE THE FORM?

The form can be completed by SHO medical staff, Staff Grade, Associate Specialist, Consultant, Senior Clinical Managers, Heads of Nursing, Matrons, Band 6 Nurses and above, Ward Managers/Heads of Department, Senior Radiographers, Senior Heads of Therapy Services and Specialist Nurses who will be expected to be leading on pulling together a formal Capacity Assessment and Best Interest determination.

WHAT IS EXPECTED OF GENERAL RECORDING FOR STAFF?
The level of detail in general recording around Capacity and Best Interests will depend upon the specific intervention being proposed by a professional and in particular on the degree of potential impact on the person. In most interventions of a routine nature staff merely need to demonstrate that they are taking account of Capacity and Best Interests at key points within their professional practice.

If the person clearly has capacity recording could be as brief as to indicate that the “impairment” or “disturbance” does not affect the persons cognitions in regard to the intervention being proposed i. e. does not “make the person unable to make the decision”. If this is unchanged at review then this capacity would merely be noted as being unchanged from that recorded in the original assessment.

For persons without capacity for a particular decision / intervention there would be the need to include an assessment summary of capacity, who will be consulted and a summary of why a course of action is decided to be in the best interests of the person. For routine interventions such recording need not be extensive and staff can choose whether to record in case notes or whether they wish to use the more detailed form. Such recording is not expected for all decisions but around significant changes only.

WHAT SHOULD BE RECORDED FOR PERSONS WHOSE CAPACITY FLUCTUATES?
Fluctuating capacity will be an issue for many persons. In such cases staff should record in their initial assessments that this could be the case stating how their practice would change in such an event e.g. postponing therapy, liaising with key carers, recording the change in capacity and how continued intervention confers with the Best Interest checklist. The best practice will clearly be to agree the response with the person and family in advance whilst the person still has capacity.

Directorate of Surgery and Anaesthesia
Record of Competency to Obtain Consent for Cardiothoracic Surgical Procedures

Name of Junior Doctor (SpR) Year of training (if applicable) Type of post

Procedure
Date of assessment
Name of assessor (please print)
Signature of assessor
Cardiac Surgery:-
CABG

AVR
MVR/Repair
Aortic Surgery
Thoracic Surgery:-
Lung Resection
Oesophagectomy
Pleurectomy
Bronchoscopy/oesophagoscopy
VATS procedures
Mediastinoscopy

Responsibilities of assessor:-
The above doctor is competent to obtain consent from patients for the above named procedures. He/she is able to discuss the nature of the procedure including the risks/benefits and any associated information required by the patient. He/she understands that further information may be required by the patient in order for them to make informed consent. If unable to provide this information, he/she will contact the patient's consultant. He/she understands that until this is done, informed consent has not been given.

Division of Cardiology/Chest Medicine
Record of Competency in Consenting for the Cardiology Procedures

Name of Junior Doctor Type of post
(SpR, Fellow, Staff Grade) Year of training
(if applicable)

Procedure
Date of assessment
Name of assessor (please print)
Signature of assessor
DC Cardioversion
Stress test and tilt test
Closure of ASD/VSD
PTCA
Valvuloplasty
Transoesophageal echo
EP studies
PCI
Pacemaker implantation under
local anaesthesia
Pacemaker box change

Responsibilities of assessor:-

The above doctor is competent to obtain consent from patients for the above named procedures. He/she is able to discuss the nature of the procedure including the risks/benefits and any associated information required by the patient. He/she understands that further information may be required by the patient in order for them to make informed consent. If unable to provide this

information, he/she will contact the patient's consultant. He/she understands that until this is done, informed consent has not been given.

Division of Cardiology/Chest Medicine
Record of Competency in Consenting for the Chest Medicine Procedures

Name of Junior Doctor Type of post
(SpR, Fellow, Staff
Grade) Year of training
(if applicable)

Procedure
Date of assessment
Name of assessor (please print)
Signature of assessor
Pleural aspiration
Chest drain insertion
Bronchoscopy
Endobronchial ultrasound
(EBUS)
Chest ultrasound
CT guided biopsy

Responsibilities of assessor:-

The above doctor is competent to obtain consent from patients for the above named procedures. He/she is able to discuss the nature of the procedure including the risks/benefits and any associated information required by the patient. He/she understands that further information may be required by the patient in order for them to make informed consent. If unable to provide this information, he/she will contact the patient's consultant. He/she understands that until this is done, informed consent has not been given.

APPENDIX I

Key Clinical Skills and Competencies for Clinical Nurse Practitioners (CNP's) to gain informed consent for Percutaneous Coronary Intervention (PCI)

Competency 8

The first section details dates that the CNP has attended catheter lab and observed PCI procedures The second section details knowledge gained in reading up to date relevant consent literature.
The third section details the CNP observing other professionals deemed competent in the process of obtaining consent from patients The fourth section details the CNP being supervised / observed gaining consent from patients.
The final section details the assessment of the CNP in obtaining consent.

Section 1 – Details dates that the CNP has attended Catheter lab' and observed a minimum of 3 PCI procedures Please see the specific important observations you must consider, listed in the appendix 1.

Date
State procedures observed and number of times
Signed by lab

Section 2 - Details knowledge gained in reading up to date relevant consent literature e.g.

Date Appropriate material read / study days
National – Department of Health (2001), Good Practice in Consent Implementation Guide: Consent to Examination or Treatment. Nursing Midwifery Council guidance on consent (2007).
Local – CTC consent policy, CTC CNP consent protocol, Sedation Policy, Attend risk management day, attend consent study day
12 key points on consent: The Law in England DOH 2001

Evidence of reflection / dates

APPENDIX J

Key Clinical Skills and Competencies for Clinical Nurse Practitioners (CNP's) to gain informed consent for Permanent Pace Makers (PPM) Insertion & / PPM Generator Replacement (Box Change)

Competency 7

The first section details dates that the CNP has attended pace-maker theatre and observed the implantation of pace-maker / box change / reveal The second section details knowledge gained in reading up to date relevant consent literature e.g. CTC policy / National guidelines / study day The third section details the CNP observing other professionals deemed competent in the process of obtaining consent from patients
The fourth section details the CNP being supervised / observed gaining consent from patients.

The final section details the assessment of the CNP in obtaining consent.

Section 1 – Details dates that the CNP has attended pace-maker theatre and observed the implantation of pace-maker / box change / Reveal

Date
Procedure observed e.g. PPM, box change, reveal

APPENDIX K

Directorate of Cardiology and Chest Medicine Record of Competency in Consenting for Tilt Testing

Name (print) Type of post
(Specialist Clinical Practitioner/Associate Practitioner) Signature

Procedure	Date of assessment	Name of assessor (please print)	Signature of assessor
Tilt Testing			
1.			
2.			

Responsibilities of assessor:-

Upon completion of the above assessments, the Specialist Clinical Practitioner/Associate Practitioner is competent to obtain consent from patients for the above named procedure. He/she is able to discuss the nature of the procedure including the risks/benefits and any associated information required by the patient. He/she understands that further information may be required by the patient in order for them to make informed consent. If unable to provide this information, he/she will contact the patient's consultant. He/she understands that until this is done, informed consent has not been given.

APPENDIX L

Policy to be read in conjunction with the following documents

Incident reporting policy Mental Capacity Act Correct site Surgery Policy
GMC obtaining Consent Procedure Clinical Nurse Specialist PCI protocol
Clinical Nurse Specialist Pacemaker protocol Vulnerable Adult Policy
Information policy re leaflets

8. Endorsed By:

Name of Lead Clinician / Manager or Committee Chair	Position of Endorser or Name of Endorsing Committee	Date
Raj Jain	Chief Executive	Sept 2008

9. Record of Changes

Section No	Version No	Date of Change	Description of Amendment	Description of Deletion	Description of Addition	Reason
9.0 9.1 9.2	Process for identifying staff who are not capable of performing the procedure but who are authorised to obtain consent	NIL	Change of wording to ensure compliance with NHSLA minimum criteria.	Clarification of process required	9.0 9.1 9.2	Process for identifying staff who are not capable of performing the procedure but who are authorised to obtain consent
17 17.1 17.2	Training requirements	Nil	Change of wording to ensure compliance with NHSLA minimum criteria.	Clarification of process required	17 17.1 17.2	Training requirements
Appendix H	Competency requirement forms	Nil	To comply with NHSLA minimum criteria	Ensure appropriate documentation for recording competency for obtaining consent.	Appendix H	Competency requirement forms

Record of Changes to Document - Issue number: 2.4	
Changes approved in this document:	**Date: Nov 2011**

Section Number	Amendment	Deletion	Addition	Reason
Appendix m	Competency requirement forms	Nil	To comply with NHSLA minimum criteria	Ensure appropriate documentation for recording competency for obtaining consent.
9.3			Section on Specialist Clinical Physiologist undertaking consent for tilt testing procedure –added to the policy, following consultation with Dr N Palmer, Consultant in Cardiology and Julie Henderson, Specialist Clinical Physiologist.	Additional staff who will undertake consent for a specified procedure
9.4	Process for following up those who have obtained consent for a procedure without being authorised to do so.	Nil	To comply with NHSLA minimum criteria	Clarification of process required

Record of Changes to Document - Issue number: 2.6				
Changes approved in this document:			**Date: July 2018**	
Section Number	Amendment (***shown in bold italics)***	Deletion	Addition	Reason

10.1	Bayley v George Eliot Hospital	Nil	2nd paragraph	To emphasize need to provide all treatment options as per Trust Solicitors advice
10.2	Montgomery and Informed Consent	Nil	This whole section has been added including other relevant case law as per the Trust Solicitors	This is a landmark case for informed consent in the UK
8.0	This section has been modified from 2nd para on page 9 to provide greater explanation	Nil	2nd para p9 onwards added	This came up in the review from the Trust Solicitors
18.0	This is a new section on infections associated with heater cooler units / Mycobacterium chimaera	Nil	The whole section	This is a new issue since the last consent policy was ratified and reflects guidance from PHE
19.0	This was the old section 18 and has now become section 19	Nil	The old section 18 has now become this section 19	Section 18 now dedicated to HCU- associated infections

Record of Changes to Document - Issue number: 2.7	
Changes approved in this document:	**Date: 7th May 2021**

Section Number	Amendment (***shown in bold italics)***	Deletion	Addition	Reason
9.5 17.2 17.3	Specialist Nurses employed within cardiology will be identified as able to obtain consent for specific procedures as agreed by the clinical lead.	Nil	Addition of cardiology specialist nurses to list of those able to consent.	Additional staff who will undertake consent for specified procedures.

Health Records Management

Policy

For completion by Author			
Author(s) Name and Title:	Wyn Taylor, Head of Information Governance & Administration		
Scope:	Trust Wide	Classification:	Non-Clinical
Version Number:	6.0	Review Date:	26/06/2024
Replaces:	5.1		
To be read in conjunction with the following documents:	Data protection policy Information Governance Strategy Information Governance Policy Information Security Management System (ISMS) Health Records Scanning Procedures Data Quality Policy Information Disclosure Policy Clinical Record Keeping Policy Patient Identification Policy Document Control Policy Code of Conduct for HandliFng Personal Data Records Management: Code of Practice for Health and Social Care		
Document for public display:	Yes		
Executive Lead	Kate Warriner		

For completion by Approving Committee			
Equality Impact Analysis Completed:		Yes	
Endorsement Completed:	Yes	Record of Changes	Yes
Authorised by:	IT Operations Group	Authorisation date:	26/06/2021

For completion by Document Control					
Unique ID No:	TC10(08)	Issue Status:	Approved	Issue Date:	30/07/2021
After this document is withdrawn from use it must be kept in archive for the lifetime of the Trust, plus 6 years.					
Archive:	Document Control		Date Added to Archive:		
Officer responsible for Archive:	IG and Document Control Facilitator				

Contents

Document Statement

Liverpool Heart & Chest Hospital NHS Foundation Trust's objective is to ensure that the management of health records within the organisation, from creation to their eventual disposal is done within guidelines that comply with legislation, national requirements and best practice.

Health records are a key foundation upon which patient care; quality information and successful management of patients depend upon. The accuracy, timeliness and availability of the health record in electronic and manual form is key to delivering high quality services offered to patients.

This policy provides guidance for all staff regarding the creation, maintenance, safe-keeping (confidentiality and security) of health records.

Records Management is the process by which an organisation manages all aspects of a record in any format or media type, throughout the lifecycle of the record.

The Records Management Code of Practice for Health and Social Care published by NHSX is a guide to the required standards of practice in the management of records. It is based on legal requirements and professional best practice. The Trust's health record provides evidence of actions and decisions taken in respect of any episode of care for an individual patient.

This Policy relates to all patient health records held in any format or media. This policy outlines the standards to be complied with, however it is acknowledged that services managing various components of patient health records should also have documented policies and processes for the management of record collections 'owned' by that service.

In this policy, health records are defined as recorded information pertaining to patient care, in any form / media type, created / received and maintained by the Trust. They are referred to as health records, EPR, EDMS Scanned Images, EMIS, medical records or case notes.

Health Records may consist of:

- Patient health record specific to NHS funded care and private patient care (electronic or paper based)
- X-ray and imaging reports, output and images
- Microfilm (fiche/film)
- Audio and video-tapes, cassettes, CD-ROM etc.
- Computerised or digital records (held on systems or information assets)

The Trust's records are an important form of information, record management is a discipline which utilises an administrative system to direct and control the creation, distribution, filing, storage, retention, archiving and disposal of records.

The key components of records management are:

- record creation
- record keeping
- record maintenance
- tracking of record movements
- access and disclosure

- closure and transfer
- archiving in house or by external third party

1. Roles and Responsibilities

Chief Executive

As accountable officer, the post holder is responsible for ensuring appropriate records management systems are in place to support service delivery, patient care, safety and continuity of care. Records management is key to this as it will ensure appropriate, accurate information is available as and when required.

Caldicott Guardian

Responsible for promoting a culture of confidentiality in the Trust and to act as the conscience" of the organisation in respect of maintaining patient confidentiality.

SIRO

Responsible for ensuring that an overall culture exists that values and protects information within the Trust including health records.

Head of Information Governance & Administration

Responsible for the overall development and maintenance of health records management practices throughout the Trust, in particular for drawing up guidance for good health records management practice.

All Staff

All Trust staff, whether clinical or administrative, who create, receive or use health records have record management responsibilities. In particular, staff must ensure that they keep accurate records of their work in the Trust and manage those records in accordance with this policy. All staff have a duty to adhere to statutory requirements.

IT Operational Group

IT Operational Group will be responsible for reviewing and ratifying the policy.

2. Controlled Document Standards

The aim of a record management system is to ensure:

- **records are available when needed** - from which the Trust is able to form a reconstruction of activities or events that have taken place

- **records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist

- **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records

- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated

- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format

- **records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required

- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.

The Record Management Code of Practice for Health and Social Care requires that each NHS organisation should have in place a policy on how it manages, all of its records including electronic records.

The key statutory requirement for compliance with records management principles is the Data Protection Act 2018 (DPA 2018) and each NHS organisation is required to comply with its requirements. The act provides a broad framework of general standards that must be met and considered in conjunction with other legal obligations.

Under the DPA 2018 and UK General Data Protection Regulation (UK GDPR) the data protection principles set out the main responsibilities for organisations processing personal data. Personal data must be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes **and** not further processed in a manner that is incompatible with those purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Confidentiality of Information

The Trust will only collect any necessary data lawfully, fairly and accurately. It must only be held and used for specified purposes and may be accessed, altered, disclosed or destroyed only with proper authority. Authority must be given by the consultant responsible for the patient or the Caldicott Guardian.

All Trust employees must comply with the data protection arrangements appertaining to their post; this requirement is included in all new and existing employees' contracts of employment.

If there are any incidences of breaches to confidentiality of information or the Data Protection Act then this must be reported as an incident by using the Datix incident reporting system.

Caldicott Principles

All patient records are subject to the Caldicott principles. The Department of Health recommends that NHS organisations should be held accountable through governance procedures for continuously improving confidentiality and security procedures governing access to and storage of clinical information.

When transferring information about a patient to another NHS organisation, only pertinent and relevant information should be disclosed and the information should be relayed in a secure and safe manner in line with approved Trust policy.

Access to Health Records

- Patients have a right of access to health information about themselves. Access to health records of living patients is governed by the Data Protection Act 2018.
- Access to health records of deceased patients is governed by the Access to Health Records Act 1990.
- The Information Disclosure Policy details the Trusts procedures and guidelines for sharing and disclosing patient information.

NHS Guidelines and Other Standards

- Caldicott Principles
- Records Management: Code of Practice for Health and Social Care
- NHSLA Standards for Acute Trusts
- Confidentiality: NHS Code of Practice

3. Procedure

This section covers the procedures for health records specifically for:

- Creating Health Records
- Retrieving Health Records
- Tracking
- Tracing missing Health Records
- Culling / archiving of Health Records
- Creating temporary Health Records

- Merging existing Health Records
- Returning Health Records

Referrals come into the Trust from a number of sources. Local Standard Operating Procedures are in place outlining the correct processes to be followed within each service.

Staff who process the referrals will firstly check to see if the patient has already been treated at the hospital and is already a known patient and registered on the Trust PAS.

Process for Creating Health Records

All new patients to the Trust must be registered onto the Trust PAS Integrated Care System (iCS). The patient will be allocated a Master Patient Index (MPI) number. Since June 2013, no new physical case notes are made up for the patient as an Electronic Patient Record (EPR) and Electronic Document Management System (EDMS) is now utilised to document and manage patient documentation.

There are also a number of other systems and information assets utilised to manage healthcare of patients, including EMIS for Community Services, CRIS for Radiology and a number of other systems as recorded in the Trust Information Asset Register.

Each system must have appropriate Standard Operating Procedures in place to ensure appropriate records management practices to comply with legal and regulatory compliance. Information Asset Owners are responsible to ensure appropriate documentation and training is in place for all staff to follow.

Retrieving Health Records (Case Notes/Health Records for Scanning)

If a patient is due to attend for elective activity, the patients physical 'legacy' case note will be obtained and scanned in to the EDMS. This process is managed on a daily basis by the Health Records Team via reports generated from the data warehouse to ensure elective patients have records available at point of contact. A similar monitoring process will be implemented to ensure non elective patients records are retrieved and scanned in a timely manner.

Outpatient Clinics / Elective Admissions – Health records are pulled, prepped, scanned and quality assured in preparation for the patient activity and are therefore available to view in the EDMS tab of EPR.

Non-urgent requests – Non urgent requests for notes to be scanned i.e. for non-patient activity, research and audit etc, should be submitted to the health records team. The request will be assessed and prioritised accordingly.

Emergency / Non Elective Admissions / Walk In's – admissions for Primary Percutaneous Coronary Intervention (PCI) during normal working hours should be notified to the Health Records Team of the patient has a historical case note which is not already scanned.

If a patient is new to the Trust, the steps outlined in the 'Creating Health Records' section should be followed.

Tracking Health Records

Any movement of a physical case note must be tracked appropriately on PAS. If a casenote is tracked to 'ESCO' or 'Scanned' then the notes will be available in EDMS. Any queries should be directed to the Health Records Team.

Any notes returned from Off Site Storage should be tracked in as received and once scanned tracked as above.

Exceptions to the tracking process are as follows:

- Purple Inpatient and Orange Outpatient Continuation Folders are not tracked. For all patient activity, a 'paper light' continuation folder is created to store any paper documentation created during the patient episode of care. Inpatient folders are scanned at point of discharge and Outpatient folders scanned following the clinic session.
- Details on the preparation processes and use of continuation folders will be documented in Standard Operating Procedures and reviewed annually.

Tracing Unavailable Health Records

- Once a health record has been identified as unavailable, the member of staff should notify the Head of Information Governance & Administration immediately.

- Once all options and searches have been exhausted and the notes are unable to be located, the details should be entered immediately on to the unavailable casenote log and searches conducted routinely in an attempt to locate the missing notes.

- If the notes are unavailable for any subsequent activity, this should be reported and logged on Datix as an incident

Temporary Health Records

Temporary case notes are no longer created for patients since deployment of the EPR and EDMS solution.

As noted in the 'Tracking Health Records' section, a continuation folder is created for all patient activity with any paper output stored securely in the folder and returned for scanning. The Trust will maintain documented procedures for the use of the folders.

Merging Health Records

This process should only be completed by the Health Records Team, however if required can be performed by the Data Quality Manager or EPR Team. ***This process should only authorised once sufficient checks have been performed to satisfy that the record is a duplicate.***

If a duplicate record is identified, the PAS records must be merged to ensure a complete record is available. If the original and duplicated case notes have not been scanned, they should be merged together ensuring chronology of dates. The patient records should then be merged on PAS and the records scanned to the primary MPI number. The original health record will be marked as "live" on the tracking system, and tracked to its current location, and the temporary health records marked as inactive.

If the original and duplicated records have already been scanned under separate MPI's, the records can be merged in PAS which will automatically merge and re-index the patients EPR and EDMS records.

Duplicate Health Records

PAS iCS does not allow more than one patient to have the same Master Patient Index (MPI) number. Therefore, a new MPI number is created every time a new patient is registered onto the system.

Occasionally incorrect data e.g. incorrect spelling of surname or date of birth, may cause one patient to be registered again, thereby creating an additional MPI number and a duplicate physical record.

To minimise the risk of creating duplicate records for the same patient, the Data Quality Function will instigate traces through the demographics Batch Service (DBS). The NHS number verification and validation process will help to identify any potential duplicate records.

Process for Retaining (Archiving) and Disposing of Records

All health records within the Trust are stored, distributed and processed in accordance with relevant legislation and guidance:

- Data Protection Act 2018
- Caldicott Principles
- Information Security Management Standards ISO27001
- LHCH Code of Conduct for Handling Personal Data
- Records Management: Code of Practice for Health and Social Care

The Trust is obliged under the Public Records Act 1958 to ensure the safe keeping of personal records that it retains. Notes that are to be sent for archiving will be subject to the Department of Health guidance issued in the "NHS Retention and Disposal Schedule' – Records Management: Code of Practice for Health and Social Care".

Trust Retention Periods for Health Records – When a health record is no longer required for operational purposes and the retention period has been met, the Trust currently preserves the health record indefinitely for 'living' patients. The Trust will however progress with appraising records of deceased patients in order that the case note estate can be depleted to reduce storage requirements and cost.

Any proposal for destruction of case notes will be documented for approval by the relevant senior committee including the authorisation of the Trust Caldicott Guardian and SIRO.

Archiving (retaining) of Health Records

If there is an identified requirement to archive a patient's health records i.e. those where the retention period has been met, the records will be scanned to the EDMS to maintain the integrity and availability of the record.

Process for Archiving Health Records

If a requirement is identified to archive a physical set of patient records in hard copy format, the Trust utilises an off-site storage facility under contract where the notes can be retained securely. Such requests for archive should be forwarded to the Head of Information Governance & Administration. Any submission of documentation to the off-site facility will be managed by the Health Records Team.

Process for retrieving Health Records from offsite storage

Requests for health records from offsite storage should be made via a Health Records Team.

Requests for archived notes to be extracted and uploaded to EDMS from the historical CD and DIP Systems should be forwarded to the Health Records Team.

If notes are required for elective or non-elective activity, the Health Records Team will automatically recall the patient record for scanning as detailed in the 'Retrieving Health Records' section.

Electronic Records

The principles of good records management described in this policy apply equally to records created electronically. The Trust will ensure that electronic data is managed in a manner to prevent any corruption or deterioration.

Details of the standards applied to the scanning of documentation are outlined in the Health Records Scanning Standard Operating Procedures and other associated policies and training materials via the EPR Team.

A review of system functionality, records management processes and risk assessment should be undertaken on all information assets by the respective Information Asset Owner / Administrator to ensure processes are in place to manage the data appropriately.

Health Record Security and Storage

All health records must be stored in a secure, lockable area with restricted access to authorised staff only. Adequate measures should be taken in all instances to ensure no potential damage or loss to health records, either in paper or electronic format.

Any movement or destruction of health records must be recorded on the PAS iCS tracking system. It is the responsibility of all staff to record the movement and location of health records to ensure records are always traceable.

Health records must never be left unattended, on reception desks, or any other areas where they can be easily accessed by unauthorised persons.

It is not the Trust's normal policy to send out original health records to other Trusts. This would only be considered if there was adequate justification and essential to the continuing care of the patient. This decision would be made by the consultant responsible for the patients care or by the Caldicott Guardian. In all other instances, a copy of the original health record should be made and be sent in accordance with Caldicott Principles and the Data Protection Act 2018. If health records are required for legal reasons, clearance should be sought from the Caldicott Guardian and the Trust Data Protection Officer (Head of Information Governance & Administration).

Best Practice

The standards for clinical record keeping are outlined in the Trust Clinical Record Keeping Policy and associated policies on the Trust intranet.

When scanning documents into an electronic records management system, the Standard Operating Procedures for the Scanning of Health Records should be followed to ensure the principles for the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008) or BS 10008 are supported.

Training

All new staff employed to the Trust who are provided with PAS access will undergo specific training.

All new health records staff will be provided specific localised training on health records process which are documented in Standard Operating Procedures.

All staff employed by the Trust must attend the corporate induction training programme, within which the Information Governance component covers health records principles.

4. Policy Implementation Plan

The Head of Information Governance & Administration is responsible for the implementation of this policy.

The policy will be made available to all staff via the Trust Intranet and will be promoted to all staff attending the Trust corporate induction.

The IT Operational Group will be responsible for review and ratification of this policy.

Implementation of the Health Records and Case Note Management Policy will aid the Trust to:

- Demonstrate compliance with the records management and health records specific components of the Data Security and Protection Toolkit (DSPT) annual submission.
- Support the Liverpool Heart and Chest Hospital Patient Vision by ensuring patient health records are maintained confidentially, retain integrity and are available when required.
- Support legal and statutory compliance in line with legislative and professional standards.

5. Monitoring of Compliance

The Trust will commission annual audits, both internal and external, to monitor the effectiveness of compliance with the Trust processes linked to Information Governance and information security.

Internal and external audits will be reviewed by the IT Operational Group and where applicable the Trust Audit or Risk Committees.

6. References

Data Protection Act 2018/ UK General Data Protection Regulation

Records Management Code of Practice for Health and Social Care

Caldicott Principles

Access to Health Records Act 1990

NHSLA Standards for Acute Trusts

Confidentiality: NHS Code of Practice

Information Security Management Standards ISO27001

LHCH Code of Conduct for Handling Personal Data

Public Records Act 1958

Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008)

7. Appendices

8. Endorsed By:

Name of Lead Clinician / Manager or Committee Chair	Position of Endorser or Name of Endorsing Committee	Date

9. Record of Changes

Section No	Version No	Date of Change	Description of Amendment	Description of Deletion	Description of Addition	Reason
Document Statement	5.1	26/07/21			*EPR, EMIS, EDMS Scanned Images,*	Capture all systems
1.0			*Head of Information Governance & Administration*			Amendment to responsible role
1.0			*IT Operational Group*			Governance Structure
1.0				Clinical Records Committee		Governance Structure
2.0			*Data Protection Act 2018 and principles*			Updated legislation
2.0			*Datix*			Change to Incident reporting software
2.0			*DPA 2018*			Updated legislation
2.0				CQC Outcome 21 Records Management		Updated standards
3.0			*Local Standard Operating Procedures are in place outlining the correct processes to be followed within each service.*			Reference to SOP's rather than detail in Policy
3.0					There are also a number of other systems and information assets utilised to manage healthcare of patients, including EMIS for Community Services, CRIS for Radiology and a number of other systems as recorded in the Trust Information Asset Register. Each system must have appropriate Standard Operating Procedures in place to ensure appropriate records management practices to comply with legal and regulatory compliance. Information Asset Owners are responsible to ensure appropriate documentation and training is in place for all staff to follow.	Inclusion of additional services and systems, reference to local SOPs and IAO responsibility
3.0				Detailed process of records creation in PAS		Included in specific PAS SOP's
3.0				References and processes linked to health records library		No library exists on site
3.0			*Head of Information Governance & Administration*			Amendment to responsible role
3.0				Health Records Library references		No library exists on site

3.0					If the notes are unavailable for any subsequent activity, this should be reported and logged on Datix as an incident.	New incident reporting software
3.0			*DPA 2018*			Updated legislation
3.0				Scanning Policy		No policy – local SOP's
3.0			*Head of Information Governance & Administration*			Amendment to responsible role
3.0					A review of system functionality, records management processes and risk assessment should be undertaken on all information assets by the respective Information Asset Owner / Administrator to ensure processes are in place to manage the data appropriately.	Align with IG DPIA and IAO requirements
3.0				Health Records Library references		No library exists on site
3.0					When scanning documents into an electronic records management system, the Standard Operating Procedures for the Scanning of Health Records should be followed to ensure the principles for the 'Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically' (BIP 0008) or BS 10008 are supported.	Reference to scanning standards followed for legal compliance
3.0				References to casenote tracking		No required Trust wide – process now relates only to scanning bureau
4.0			*Head of IG & Admin / IT Operational Group/ DSPT*	CQC Outcome 21		Change to job title and governance structure, and standards
5.0			*IT Operational Group*	Clinical Records Committee		Governance structure
All			Section numbering changed			To align with DC policy/current template
All			Changed name for NHS Code of Practice			Title changed in newest version released

Information Disclosure

Policy

For completion by Author			
Author(s) Name and Title:	Carol Taylor, Information Governance Manager		
Scope:	Trust Wide	Classification:	Non-Clinical
Version Number:	6.0	Review Date:	30/06/2023
Replaces:	Information Disclosure v5.0		
To be read in conjunction with the following documents:	Data Protection Policy, Information Governance Strategy, Information Governance Policy, Health Records and Case Note Management Policy, Corporate Records Management Policy, National Data Opt-out Procedure		
Document for public display:	Yes		
Executive Lead	Karen Warriner		

For completion by Approving Committee			
Equality Impact Analysis Completed:		Yes	
Endorsement Completed:	Yes	Record of Changes	Yes
Authorised by:	Operational IT Group	Authorisation date:	26/07/2022

For Corporate Governance Manual documents			
CGM Reference	B10	CGM Review date:	July 2023
Authorised by:	The Board	Authorisation date:	26/07/2022

For completion by Document Control					
Unique ID No:	TF09(10)	Issue Status:	Approved	Issue Date:	20/09/2022
After this document is withdrawn from use it must be kept in archive for the lifetime of the Trust, plus 6 years.					
Archive:	Document Control		Date Added to Archive:		
Officer responsible for Archive:	IG and Document Control Facilitator				

Contents

Document Statement

The Liverpool Heart and Chest Hospital NHS Foundation Trust (the Trust) recognises the importance and consequence of the disclosure of information, be it personal identifiable data or corporate information. The Trust complies with national legislation and best practice guidelines and ensures that information held within the organisation is disclosed in an appropriate and timely manner.

The legislation and practice defined within this policy outlines the Trust's policy and process in the holding and disclosing of information. Compliance with this policy ensures that any information leaving the Trust adheres to the principles of the defined legislation.

1. Roles and Responsibilities

The **Chief Executive** is accountable for the Trust's compliance with this policy through the work of the Digital Excellence Committee (DEC) and other associated committees as part of the Trust governance framework.

The **Chief Digital and Information Officer (CDIO)** is responsible for the implementation of the contents of this policy and is also accountable as the Trust's **Senior Information Risk Officer (SIRO)** and will be responsible for the appropriate disclosure of Trust information through the implementation of the procedures detailed within this policy.

The **Information Governance Team (IG Team)** is responsible for coordinating and responding to:-

- Subject Access Requests including miscellaneous requests, requests from the Police, requests for CCTV images, requests submitted by the Parliamentary and Health Service Ombudsman (PHSO) in relation to complaints involving other healthcare organisations
- Freedom of Information requests for corporate information
- Continuance of Healthcare requests for health record information
- Post mortems requests for health record information

The **Legal Services Team** is responsible for coordinating and responding to subject access requests relating to claims against the Trust and for release of health records in relation to Coroner requests for information and Coroner inquests.

The **Patient & Family Support Team** is responsible for coordinating and responding to Parliamentary and Health Service Ombudsman (PHSO) relating to complaints against the Trust.

The **PR & Communications Team** is responsible for coordinating and responding to 'media requests' for corporate information.

All staff must work within the guidelines of the Trust's Equality and Diversity Strategy with regard to the treatment of fellow employees. The information within this policy may be made available to speakers of other languages through the translation service available through the Patient and Family Support Team.

All staff are responsible for co-operating with the development and implementation of corporate policies as part of their normal duties and responsibilities.

Temporary or agency staff, contractors, students or others will be expected to comply with the requirements of all Trust policies applicable to their area of operation.

2. Controlled Document Standards

The Data Protection Act 2018 (DPA 2018) incorporates the UK General Data Protection Regulation (UK GDPR) and regulates the collection, processing and disclosure of personal data. The aim of the legislation is to protect individuals about whom personal data is held, to give them access to such information, and to establish a supervisory body. The Information Commissioners Office (ICO) is the UK's supervisor authority that is responsible for governing Data Protection compliance.

Under the DPA 2018/UK GDPR, processing of data is widely defined 'as any operation or set of operations performed on personal data or sets of personal data'. This includes obtaining, recording, holding, altering, retrieving, destroying or disclosing data.

Under the DPA 2018/UK GDPR, the Trust is defined as a Data Controller. A data controller determines the purposes and means of processing personal data.

The DPA 2018/UK GDPR regulates the processing, including the disclosure, of information about identifiable living individuals. Subject to specified exemptions the Regulation requires data controllers like the Trust to comply with the data protection principles as below.

The DPA 2018/UK GDPR states that personal data must be:

(a) Processed lawfully, fairly and in a transparent manner
(b) Collected for specified, explicit and legitimate purposes
(c) Adequate, relevant and limited to what is necessary
(d) Accurate and where necessary kept up to date
(e) Kept in a form which permits identification of data subjects for no longer than is necessary
(f) Processed in a manner that ensures appropriate security of the personal data

These principles are detailed in Article 5 of the DPA 2018/UK GDPR.

Information sent outside of the Trust by fax, post, e-mail or verbally over the telephone must comply with the guidance as detailed in the Trust's Information Security Management System and other relevant information governance policies and procedures.

2.1 Best Practice - Caldicott Report

Access to personal data should be on a need-to-know basis and should be in line with the principles of the Caldicott Report. The original report was commissioned in 1997 to promote good practice in handling of patient confidentiality within the NHS.

The Caldicott Review Two (Information to Share or Not to Share?) followed in March 2013 and focused on information sharing to ensure an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care. The principles of the reports are as follows and all information disclosures, flows and processing must be assessed against them:

1. Justify the purpose(s) for using patient data
2. Do not use patient-identifiable information unless it is absolutely necessary
3. Use the minimum necessary patient-identifiable information
4. Access to patient-identifiable information should be on a need-to-know basis
5. Staff should be aware of their responsibilities to maintain confidentiality
6. Staff should understand and comply with the law, in particular the DPA 2018/UK GDPR
7. The duty to share information can be as important as the duty to protect patient confidentiality

Access to personal data shall be controlled through individual system user passwords. The Trust's Information Security Management System details the procedures for the creation of accounts to access individual Trust systems. Each system will be owned by an Information Asset Owner who will be responsible for the maintenance of an up to date list of users with access to the relevant systems.

Trust staff, external contractors and healthcare researchers and consultants should only have access to such data as is required for the performance of their duties.

3. Procedure

Patient Information Communication – Strategic Aims

In line with the requirements of principle one of the DPA 2018/UK GDPR, the Trust will work to educate all staff on the fair processing of personal information via Data Security & Protection mandatory training sessions and regular communications.

Printed fair processing information / privacy notices will work in conjunction with the information explained to patients by clinicians during appointments. Information leaflets will be available in appropriate patient areas around the Trust and on Wards.

Information will also be available on the Trust's internet site. Work on patient communication materials will be carried out in conjunction with the Patient and Family Support Team and PR & Communications departments to ensure patient communications fall in line with other Trust information.

The Trust will actively promote fair processing and make the information required by Articles 13 and 14 of the GDPR available to patients regarding the processing of their personal data – see Appendix 1.

All new processing activities must be approved before processing begins via the New Data Processing Approval process.

3.1.1 Consent for processing of personal data

If consent is identified as the most appropriate lawful basis for processing personal data for a specific purpose, then consent will be obtained in line with the conditions of consent requirements set out in Article 7 of the DPA 2018/UK GDPR.

The DPA 2018/UK GDPR sets a high standard for consent and provides a specific right for individuals to withdraw their consent. Consent under the DPA 2018/UK GDPR needs to be a positive opt-in; explicit consent needs to be a clear and specific statement of consent; the use of

pre-ticked opt-in boxes; opt-out boxes or other defaults is banned; and separate consent options must available for different processing activities carried out.

Departments must develop and maintain procedures for obtaining, recording and managing consent where consent is the lawful basis supporting data processing. Procedures must include the withdrawal of consent, regular reviews and the refreshing of consent.

Requests to withdraw consent must be actioned as soon as possible.

If a patient no longer wishes their information to be processed for the specified purpose, the member of staff concerned must clarify the reasons for processing and the possible implications of removing the consent. Should a patient still wish to withdraw their consent to prevent processing (including sharing) of their information then this must be recorded in the patient's records and they should be directed to the Information Governance Team who will initiate the Data Processing Requests procedure.

Any patients asking questions relating to the uses of their information which staff cannot answer appropriately must be directed to an appropriate person, for example the Service Lead, the Patient and Family Support Team or Information Governance Team.

If personal information is to be used for a new purpose outside the original processing purpose as detailed in the fair processing (privacy notice) information leaflets and associated policies, the member of staff proposing the use of this data must identify the lawful basis being relied on to support the new processing. Where this is consent, they must explain to the data subject the new use of the information and gain their explicit consent to do so. This consent should be held by the person leading the proposed data use; details of the new data processing must however be notified to the Information Governance team for inclusion in the fair processing privacy notice.

3.1.2 National Data Opt Out

The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in the 2016 Review of Data Security, Consent and Opt-Outs.

Health and care organisations are required to comply with the national data opt-out before the compliance deadline of 31 July 2022. Once compliant, confidential patient information must not be used or disclosed before it has been assessed and national data opt-outs applied when necessary.

The Trust has declared compliance and effective from 1 April 2022 patient registered choices will be applied. The Trust's process to ensure all relevant data is cross referenced with the National Opt-Out Service datastore for in-scope activities is set out in the National Data Opt Out Procedure available on the intranet.

Access to Health Records and Personal Data Procedures

3.2 Living Patients' Health Records

3.2.1The DPA2018 / UK GDPR and health records

The DPA2018 / UK GDPR gives individuals, known as data subjects, or their authorised representative, the right to apply to see and have access to personal data held about them, including health records. These rights are known as the “Right of access by the data subject” or “subject access rights” and are contained in Article 15 of the Regulation.

Data Protection legislation defines a health record as a record consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual.

A health record can be recorded in computerised or manual form or in a mixture of both. It may include such things as hand-written clinical notes, letters to and from other health professionals, laboratory reports, radiographs and other imaging records such as x-rays and not just x-ray reports, printouts from monitoring equipment, photographs, videos and tape-recordings of telephone conversations.

3.2.2 Receiving an access request under the DPA2018 / UK GDPR

Under the DPA2018 / UK GDPR, individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information, namely the information that should be provided in the Trust’s fair processing privacy notice

A request for access to health records should be made in writing, which includes by email. Application forms are available on the Trust’s internet, intranet and from the IG Team upon request.

All requests from patients or from solicitors acting on behalf of patients must be date stamped and forwarded immediately as follows:

1. Requests from patients or solicitors acting on their behalf to the IG Team
2. Requests from solicitors regarding legal claims against the Trust to the Legal Services Team

Irrespective of the type of request the principles outlined in this section of the policy will be adhered to.

The Applicant should provide enough proof to satisfy the Trust of their identity and to enable the Trust to locate the information required. If this information is not contained in the original request the Trust should seek proof as required.

Where requests are made on behalf of the individual patient the Trust should be satisfied that the patient has given consent to the release of their information.

As good practice the Trust may check with the Applicant whether all or just some of the information contained in the health record is required before processing the request. This may eliminate unnecessary work by NHS staff however, there is no requirement under the Regulation for the Applicant to inform the data controller of which parts of their health record they require.

Where an access request has previously been met the DPA2018 / UK GDPR permits that a subsequent identical or similar request does not have to be fulfilled unless a reasonable time interval has elapsed between.

When determining what a reasonable time period is for submission of another similar request the Trust will consider the following:-

- The complexity of the request
- The relationship between to Trust and the data subject
- The background / context of the request etc.

Requests for information received from the police are processed under the provisions of the DPA2018 / UK GDPR.

Police requests received during office hours (08:30-16:30 Monday to Friday) should be forwarded to the IG Team for action. Police requests received outside office hours should be forwarded to the Hospital Co-ordinators. Requests will be processed in line with the Trust's Disclosure of Personal Information to the Police procedure.

3.2.3 Recording the access request

When the necessary information is obtained, the request should be recorded on internal systems and complied with within one month of receipt. In exceptional circumstances where it is not possible to comply within this period the compliance period can be extended however the Applicant should be informed within one month of the receipt of the request that this is the case, and an explanation as to why the extension is necessary must be provided.

3.2.4 Fees to access and copy health records under the DPA2018 / UK GDPR

Under the DPA2018 / UK GDPR access to personal information must be provided free of charge, however a charge may be applied to requests that are excessive or where disproportionate effort is needed to comply. A charge can also be levied to supply additional copies of information already provided.

3.2.5 Appropriate health professional to consult

The Data Protection (Subject Access Modification) (Health) Order 2000 sets out the appropriate health professional to be consulted to assist with subject access requests as the following:

- the health professional who is currently, or was most recently, responsible for the clinical care of the data subject in connection with the information which is the subject of the request; or

- where there is more than one such health professional, the health professional who is the most suitable to advise on the information which is the subject of the request.

3.2.6 Situations where health information may be limited or denied

The Data Protection (Subject Access Modification) (Health) Order 2000 enables the Trust to limit or deny access to an individual's health record where:

- the information released may cause serious harm to the physical or mental health or condition of the patient, or any other person, or

- access would disclose information relating to or provided by a third person who has not consented to that disclosure unless:

- The third party is a health professional who has compiled or contributed to the health records or who has been involved in the care of the patient.

- The third party, who is not a health professional, gives their consent to the disclosure of that information.

It is reasonable to disclose without that third party's consent.

3.2.7 Patients living abroad requiring access to their health records

Former patients of the Trust now living outside of the UK who had treatment in the UK have the same rights under the DPA2018 / UK GDPR to apply for access to their UK health records. The Trust will treat these requests the same as someone making an access request from within the UK.

Where the patient specifically requests information to support their ongoing care, their consultant may be prepared to provide a summary of the patient's treatment to provide to their new doctor. This will however be at the discretion of the individual consultant. As an alternative the patient should be informed that their new care provider can submit a Continuance of Healthcare request to the Trust instead - see Section 4.2.

3.2.8 Parental access to their child's health record

Normally a person with parental responsibility will have the right to apply for access to their child's health record. However, in exercising this right a health professional should give careful consideration to the duty of confidentiality owed to the child before disclosure is given.

The law regards young people aged 16 or 17 to be adults in respect of their rights to confidentiality. Children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence respected. However, good practice dictates that the child should be encouraged to involve parents or other legal guardians in their healthcare.

3.2.9 The release stage

Copies of the relevant parts of the health record should be provided to the patient or their representative. Alternatively, a date should be set for the relevant records to be viewed.

Where the data subject makes the request by electronic means, and unless they state otherwise, the information should be provided in a commonly used electronic form as per Article 15 of the DPA2018 / UK GDPR.

If information has been denied or restricted by the Trust an explanation for this does not have to be given to the data subject. However, the Trust should record its justification for restricting access.

Where the information is not readily intelligible to the patient, for instance abbreviations or medical terminology, then an explanation should be provided.

3.2.10 Viewing health records

If it is agreed that the patient or their representative may directly inspect their health records, it should be considered whether access should be supervised by a health professional or a lay administrator.

A lay administrator is a neutral person who can oversee the viewing and ensure that the record remains safe. In these circumstances the lay administrator must not comment or advise on the content of the record. If the applicant raises queries an appointment with a health professional should be offered.

3.2.11 Amendments to health records

Credible records are an important aid in providing safe healthcare to patients. Records should reflect the observations, judgements and factual information collected by the contributing health professional. The DPA2018 / UK GDPR fourth principle requires that information should be accurate and kept up to date. This provides the legal basis for enforcing correction of factual inaccuracies. An opinion or judgement recorded by a health professional, whether accurate or not, should not be deleted. Retaining relevant information is essential for understanding the clinical decisions that were made and to audit the quality of care.

If a patient feels that information recorded on their health record is incorrect, they should first make an informal approach to the health professional concerned to discuss the situation in an attempt to have the records amended. Where both parties agree that information is factually inaccurate it should be amended to clearly display the correction whilst ensuring that the original information is still legible. An explanation for the correction should also be added.

Where the health professional and patient disagree about the accuracy of the entry, the Department of Health recommends that the data controller should allow the patient to include a statement within their record to the effect that they disagree with the content.

3.2.12 Patient requests for raw data information

Occasionally patients will request a copy of their test results when attending clinic and while the Trust acknowledges and supports patient rights to access their data any disclosures remain subject to the requirements of the DPA2018 / UK GDPR.

Accordingly copies of test results will be provided to patients when they request it at clinic and where there is a specific justified purpose in disclosing the raw data.

The decision to disclose raw data is a clinical decision and all disclosures must be proportionate to the specific purpose. Details of the information released and the reason for the disclosure must be recorded in the patient's health record by the authorising clinician.

3.3 Continuance of healthcare requests for access to health records

Requests submitted by other healthcare organisations to support the ongoing care of patients will be processed by the IG Team in line with the Trust's Access to Health Records Requests for Continuance of Healthcare procedure.

Disclosure will be made as soon as possible in line with the following timescales:

- Standard requests within 2 to 3 working days
- Urgent requests within 1 to 2 working days although every effort will be made not to leave open over the weekend, such as requests relating to current inpatients
- Same day or 'ASAP' requests will be considered on a case-by-case basis depending on the team's workload and if the records are accessible

Requests received after 4:30pm will be deemed to be next business day work and will be processed accordingly. Requests should be made using the online request form available on the Trust's website – Online request form
Filepath - www.lhch.nhs.uk / about-lhch / information-governance / data-protection-and-confidentiality / continuance-of-healthcare-requests.

In line with data protection principles and Caldicott guidelines all disclosures will be proportionate to the individual request. Full and complete copy health records will not be provided.

3.4 Deceased Patients' Health Records

The Access to Health Records Act 1990 (AHRA) provides a small cohort of people with a statutory right of to apply for access to information contained within a deceased person's health record.

There may be circumstances where individuals who do not have a statutory right of access under AHRA request access to a deceased patient's record. Current legal advice is that the Courts would accept that confidentiality obligations owed by health professionals continue after death. The Department of Health, General Medical Council and other clinical professional bodies have long accepted that the duty of confidentiality continues beyond death and this is reflected in the guidance they produce.

In these circumstances the general rules that apply to the disclosure of confidential patient information should have effect to determine whether a disclosure is appropriate and lawful. Requests should be considered on a case-by-case basis and not simply rejected.

There are also a range of public bodies that have lawful authority to require the disclosure of health information. These include the Courts, legally constituted Public Inquiries and various Regulators and Commissions e.g. the Audit Commission and the Care Quality Commission. In these cases the common law obligation to confidentiality may be overridden. This however does not constitute an automatic right and again must be assessed on a case-by-case basis.

3.4.1 Access to Health Records Act 1990

The Access to Health Records Act (AHRA) 1990 provides certain individuals with a right of access to the health records of a deceased individual. These individuals are defined under

Section 3(1)(f) of that Act as, 'the patient's personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the executor or administrator of the deceased person's estate.

The personal representative is the only person who has an unqualified right of access to a deceased patient's record and need give no reason for applying for access to a record. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death.

There is less clarity regarding which individuals may have a claim arising out of the patient's death. Whilst this is accepted to encompass those with a financial claim, determining who these individuals are and whether there are any other types of claim is not straightforward. The decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether a claim arises the Trust should seek legal advice.

The Trust must satisfy itself as to the identity of applicants who should provide as much information to identify themselves as possible. Where an application is being made on the basis of a claim arising from the deceased's death, applicants must provide evidence to support their claim. Personal representatives will also need to provide evidence of identity.

3.4.2 Applying for access under AHRA

A request for access should be made in writing to the Trust and must contain sufficient information to enable the correct records to be identified. Applicants may wish to specify particular dates or parts of records which they wish to access. The request should also give details of the applicant's right to access the records.

Once the Trust has the relevant information the request should be complied with promptly and within 21 days where the record has been added to in the last 40-calendar days, and within one month otherwise.

Requests for access are processed centrally by the IG Team and applications should be date stamped upon receipt and forwarded directly to the team.

3.4.3 Disclosure in the absence of a statutory basis

Disclosures in the absence of a statutory basis should be in the public interest, be proportionate, and judged on a case-by-case basis. The public good that would be served by disclosure must outweigh both the obligation of confidentiality owed to the deceased individual, any other individuals referenced in a record, and the overall importance placed in the health service providing a confidential service. Key issues for consideration include any preference expressed by the deceased prior to death, the distress or detriment that any living individual might suffer following the disclosure, and any loss of privacy that might result and the impact upon the reputation of the deceased. The views of surviving family and the length of time after death are also important considerations. The obligation of confidentiality to the deceased is likely to be less than that owed to living patients and will diminish over time.

Another important consideration is the extent of the disclosure. Disclosing a complete health record is likely to require a stronger justification than a partial disclosure of information abstracted from the record. If the point of interest is the latest clinical episode or cause of

death, then disclosure, where this is judged appropriate, should be limited to the pertinent details.

This policy is not intended to support or facilitate open access to the health records of the deceased. Individual(s) requesting access to deceased patient health information should be able to demonstrate a legitimate purpose, generally a strong public interest justification and in many cases a legitimate relationship with the deceased patient. On making a request for information, the requestor should be asked to provide authenticating details to prove their identity and their relationship with the deceased individual. They should also provide a reason for the request and where possible, specify the parts of the deceased health record they require.

Relatives, friends and carers may have a range of important reasons for requesting information about deceased patients. For example, helping a relative understand the cause of death and actions taken to ease suffering of the patient at the time may help aid the bereavement process, or providing living relatives with genetic information about a hereditary condition may improve health outcomes for the surviving relatives of the deceased.

In some cases the decision about disclosure may not be simple or straightforward therefore the Trust's Caldicott Guardian or Head of Information Governance should be consulted. In the most complex cases it may be necessary to seek legal advice.

3.4.4 Fees for access to deceased patients' health records

Under the DPA2018 / UK GDPR access to personal information must be provided free of charge, however a charge may be applied to requests that are excessive or where disproportionate effort is needed to comply. A charge can also be levied to supply additional copies of information already provided.

3.4.5 Exemptions to disclosures of information relating to deceased patients

If the deceased person had indicated that they did not wish information to be disclosed, or the record contains information that the deceased person expected to remain confidential, then it should remain so unless there is an overriding public interest in disclosing.

In addition, the record holder has the right to deny or restrict access to the record if it is felt that:

- disclosure would cause serious harm to the physical or mental health of any other person;

- or would identify a third person, who has not consented to the release of that information.

Post-mortem reports are not to be disclosed unless the information has already been obtained by the Applicant through other means (eg. a copy has previously been issued directly to them by the Coroner's Office). Otherwise, if the Applicant requires a copy of the report then they must contact the relevant Coroner's Office directly.

3.5 Employee information and other personal data held by the Trust

The DPA2018 / UK GDPR right of subject access also covers requests from individuals or their authorised representative, for access to other personal information held about them by the Trust. This includes information relating to employees, volunteers and patients requesting access to personal information not held in their health record.

Requests for access must be made in writing, clearly detailing what information is required and be supported with proof of the Applicant's identity. Application forms are available on the Trust's internet & intranet and from the IG Team. The Trust does not charge for processing access to personal information requests.

Requests for access are processed centrally by the IG Team and applications should be date stamped upon receipt and forwarded directly to the team.

The IG Team will log and validate requests before gathering the requested information, the Team will contact holders of the relevant information for example HR, Payroll and local line managers.

The IG Team will review the information to establish if any information held is exempt from disclosure under the provisions of the Regulation. Exempted information includes information relating to identifiable third-party individuals and information held in connection with any actual or proposed legal proceedings.

Requests for access to Occupational Health Records must however be directed to the Trust's OH provider for processing:

Team Prevent UK Ltd
1st Floor The Steadings Barn
Pury Hill Business Park Nr
Alderton, Towcester
Northamptonshire NN12 7LS
lhch@teamprevent.co.uk

3.6 Access to Corporate Information Procedure

The Freedom of Information Act 2000 (FOI) gives individuals the general right of access to all types of "recorded" information held by public authorities (and those providing services for them), sets out exemptions from that right and places a number of obligations on public authorities.

The Trust has two main responsibilities under the Act, it must publish and maintain a "Publication Scheme", and it must respond to requests for information.

In adopting a Publication Scheme, the Trust has adopted the Scheme proposed to all NHS bodies by the Information Commissioner. The Publication Scheme is a document which outlines the structure of the organisation through the relevant links of the Trust's website and documents the classes of information the Trust holds. The scheme will be available to the public through the Trust's website and in paper copy from the Information Governance Team.

The Environmental Information Regulations (EIR) gives the public access to environmental information held by public authorities, this is done in two ways:

- public authorities must make environmental information available proactively
- members of the public are entitled to request environmental information from public authorities.

Information will be published through the publication scheme available on the Trust website

3.6.1 Requests for Information

Requests for information must describe accurately the information required and the detail must be sufficient to allow the Trust to identify and locate it. A request under Freedom of Information must be:

- In written form (paper or electronic)
- Legible
- State the name and address of the applicant for correspondence
- Describe the information required
- Be capable of being used for subsequent reference

Requests under Environmental Information Regulations can be made verbally however the Trust must respond in writing therefore the Requester's name and contact details for correspondence should be obtained along with details of the request.

3.6.2 Procedures for Dealing with Requests

Requestors who make an FOI request verbally must be asked to put their request in writing, the request should be sent to the Information Governance Team. Requesters making a verbal EIR requests should be transferred to the IG Team on 0151 600 1845.

Written requests, including emailed requests may be received by any member of staff within the Trust and from this point the 20-working day response period is activated. All requests should be passed to the IG Team who will log the request accordingly and acknowledge receipt of the request. The process of responding to the request will follow the process as detailed in Appendix 3.

Emails received between midnight and 23:59 will be deemed received during the current working day while emails received after midnight will be received and processed as next business day.

3.6.3 Complex or costly requests

There may be cases where the costs of meeting a request would exceed the appropriate limit, set at £450 by the Office of the Information Commissioner. If this is the case, the Trust is allowed to refuse to answer the request. To estimate these costs the Trust should use an hourly rate of £25 per person per hour.

In estimating whether to respond to a request would exceed the £450 limit the Trust should take into account the costs of employing staff to:

- Find out whether the information is held
- Locate and retrieve the information
- Extract the information (including editing and redacting)

3.6.4 Time Limits

The Trust must comply with a request promptly or within 20-working days from the date of the formal request. This would also include issue of a notice if a public interest exemption applies to the information.

3.6.5 Communication of Information

If a Requestor expresses a preference for the way the information requested is given to them it should be honoured, as far as it is reasonably practicable to do so.

4. Policy Implementation Plan

The Information Governance Team is responsible for the implementation of the contents of this policy.

This policy will be disseminated via the intranet and through the inclusion of its contents during staff induction, mandatory training, and departmental IG/data security and protection training sessions.

Awareness of fair processing will be through the following methods:

- Website information
- Leaflets to be distributed as appropriate around the Trust
- Data Protection; Information Governance and Information Security Management System policies published on the Trust's Policy and Procedures intranet page
- Patient and Family Support Team

5. Monitoring of Compliance

The IG Team will maintain logs of all Continuance of Healthcare; Subject Access and Freedom of Information requests received and the associated actions and response times.

Adherence to this policy will be monitored by the IG Manager and Head of Information Governance / Data Protection Officer (DPO). Regular performance reports detailing the number of requests received and compliance with legal timeframes for responses will be submitted to the Operational IT Group and Executive Team.

Complaints submitted to the ICO regarding information disclosure compliance will also be monitored.

6. References

Data Protection Act 2018 (DPA2018) / UK General Data Protection Regulation (UK GDPR)
Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000
Access to Health Records Act 1990 (AHRA)
Freedom of Information Act 2000 (FOIA)
Environmental Information Regulations 2004 (EIR)

EU General Data Protection Regulation (GDPR) - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
Section 45 Code of Practice (November 2002) under Part 1 of the FOIA 2000
Section 46 of the Freedom of Information Act 2000 (November 2002)
NHS Digital – National Opt-out website https://digital.nhs.uk/services/national-data-opt-out
National Data Guardian, Review of data security, consent and opt-outs, https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs
ICO website https://ico.org.uk/

7. Appendices

APPENDIX 1 - The right to be informed under the DPA2018 / UK GDPR

	Data obtained directly from data subject	**Data not obtained directly from data subject**
	The following information should be provided at the time data is collected:	Within a reasonable period of having obtained the data (within one month) or at the latest: ▪ If the data is for communication with the data subject then at the first communication ▪ If the data is to be disclosed to another recipient **before** first disclosure
Identity and contact details of the controller and the data protection officer (and if applicable the controller's representative)	☑	☑
Purpose and the lawful basis for the processing	☑	☑
The legitimate interests of the controller or third party, where applicable	☑	☑
Categories of personal data being processed		☑
Details of any recipient or categories of recipients of the personal data	☑	☑
Details of overseas transfers and the safeguards used to protect the data	☑	☑
Retention period or criteria used to determine the retention period	☑	☑
Existence of data subject's rights	☑	☑
The right to withdrawn consent at any time, where relevant	☑	☑

The right to lodge a complaint with a supervisory authority e.g. the UK's ICO	☑	☑
The source the personal data originates from and whether it came from publicly accessible sources		☑
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	☑	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	☑	☑

APPENDIX 2 - FOI Exemptions

The FOI Act requires the Trust in response to a request for information to state if it holds the information requested and if it does to provide the information to the applicant unless an exemption applies.

Part II of the Act (Sections 21 to 44) lists the exemptions to disclosure, they are either absolute or qualified:

- Absolute exemptions - means that if one of these eight exemptions applies there is no right to the information under Act
- Qualified exemptions - which are subject to the **Public Interest Test.** This means that the public interest in releasing the information must also be considered, see below.

Absolute Exemptions

- Section 21 - Information accessible by other means
- Section 23 - Information supplied by, or relating to, bodies dealing with security matters
- Section 32 - Information contained in court records
- Section 34 - Parliamentary privilege
- Section 36 - Prejudice to effective conduct of public affairs
- Section 40 - Personal Information
- Section 41 - Information provided in confidence
- Section 44 - Legal prohibitions on disclosure

Qualified Exemptions

- Section 22 - Information intended for future publication
- Section 24 - National security

- Section 25 - Supplimentary provisions Sections 23 & 24
- Section 26 - Defence
- Section 27 - International Relations
- Section 28 - Relations within the UK
- Section 29 - The economy
- Section 30 - Investigations
- Section 31 - Law enforcement
- Section 33 - Public audit
- Section 35 - Government policy formulation
- Section 36 - Effective conduct of public affairs
- Section 37 - Communications with her Majesty & the awarding of honours
- Section 38 - Health and Safety
- Section 39 - Environmental information
- Section 42 - Legal professional privilege
- Section 43 - Commercial Interests

With the exception of Section 21 (information available by other means) exemptions apply not only to the communication of information but also to the duty to confirm or deny, if that itself would disclose information that it is reasonable to withhold.

The Trust's procedure for handling FOI requests requires that the decision to apply exemptions and withhold information be made by the Trust's IG Manager, Head of IG and/or a nominated Executive Lead.

APPENDIX 3 – EIR Exceptions

Regulation 12 sets out the exceptions allowing organisations to refuse to disclose environmental information. All the exceptions are subject to the public interest test.

- Regulation 12(3) - personal information
- Regulation 12(4) - exceptions based on the type of information
    - 12(4)(a) - information not held
    - 12(4)(b) - the request is manifestly unreasonable
    - 12(4)(c) - the request is too general
    - 12(4)(d) - the request relates to information which is unfinished or in the course of being completed
    - 12(4)(e) - the request involves the disclosure of internal communications
- Regulation 12(5) - exceptions based on the content of the information requested
    - 12(5)(a) - international relations, defence, national security and public safety
    - 12(5)(b) - the course of justice, the ability of a person to obtain a fair trial or the ability of a public authority to conduct an inquiry of a criminal or disciplinary nature
    - 12(5)(c) - intellectual property rights
    - 12(5)(d) - the confidentiality of the proceedings of a public authority where such confidentiality is provided by law
    - 12(5)(e) - the confidentiality of commercial or industrial information where such confidentiality is provided by law to protect a legitimate economic interest
    - 12(5)(f) - the interests of the supplier of the information
    - 12(5)(g) - protection of the environment
- Regulation 12(9) - emissions

APPENDIX 4 – Process for dealing with FOI Requests

Action	By Who
1. Validate and log request on the Master FOI Log - allocate unique reference number; open request file; calculate 15 working day internal and 20 working day external deadlines.	IG Team
2. Acknowledge request using the standard email or letter template within 2-working days of receipt.	IG Team
3. Assess request to ascertain if the requested information is held and which department or departments hold the information.	IG Team
4. Request the information from relevant Head of Department or key lead using the Management Response email template.	IG Team
5. Provide Management Response information to Information Governance within six working days. - FOIRequests@lhch.nhs.uk	Head of Department / key lead
6. Chase Management Response if not received in full - 1st chaser – 7-working days after Management Response requested; 2nd – 5-working days; 3rd chaser – 4-working days	IG Team
7. Check Management Response information for accuracy and completeness. If applicable, raise queries and/or seek further guidance.	IG Team
8. Draft response letter; send for review and update Master FOI log with actions and response details.	IG Team
9. Review draft Response Letter for accuracy & completeness and identify if Senior Manager Review is required ahead of Executive sign-off.	IG Manager / Head of IG
10. Where applicable, review and approve draft response for Executive sign-off. Identify potential media interest or misinterpretation and further context added if required.	Senior manager
11. Approve and sign off response for release	Appropriate Executive or Deputy
12. Issue response to Requestor and copy to Communications team	IG Team
13. Update Master FOI log and mark closed, move correspondence from Outlook into the network folder and mark closed.	IG Team
14. Publish FOI response on the Disclosure Log website page	IG Team

8. Endorsed By:

Name of Lead Clinician / Manager or Committee Chair	Position of Endorser or Name of Endorsing Committee	Date
Andrew Carter, Interim Head of Digital Systems	Operational IT Group	23 June 2021
Leanne Fearnehough, Associate Director for Operational IT	Operational IT Group	13 July 2022

9. Record of Changes

Section No	Version No	Date of Change	Description of Amendment	Description of Deletion	Description of Addition	Reason
Cover	6.0	June 2022	Author's job title amended			To reflect change
Whole document	6.0	June 2022	Information Governance Team replaced with IG Team, LHCH replaced with the Trust			Consistency
1	6.0	June 2022	Digital Healthcare Committee amended to Digital Excellence Committee (DEC)			Committee name change
3	6.0	June 2022	National data opt out updated with new compliance deadline and Trust status			Change to deadline and Trust status
3	6.0	June 2022	Urgent COH requests reworded		Online request form detailed	Clarity
3	6.0	June 2022			Reference to EIR added	Completeness re handling of corporate information requests
3	6.0	June 2022	Timings for email requests			Alignment with ICO guidance
4	6.0	June 2022	IG training amended to IG/data security and protection			Alignment with naming convention of mandatory training
6	6.0	June 2022			Reference to EIR added	Completeness re handling of corporate information requests
Appendices	6.0	June 2022	FOI exemptions reworded with additional guidance		EIR exceptions added	Completeness re handling of corporate information requests
	6.0	June 2022	FOI process updated and presented in table format			Clarity and alignment with current process