Liverpool Heart and Chest Hospital NHS
NHS Foundation Trust

# Information Governance Staff Handbook

- Confidentiality
- Data Protection
- Freedom of Information
- Health Records
- Information Governance Management
- Information Quality Assurance
- Information Risk
- Information Security

# Table of Contents

# What is Information Governance?

Information governance contains the set of standards that the NHS must follow to make sure that it carries out its duty to:

- maintain full and accurate records of the care provided to patients
- keep patient records confidential, secure and accurate

Information governance is a framework that informs the NHS and its partner organisations of the processes and procedures that it must have to ensure:

- patient confidentiality is respected
- patient records are held in secure conditions
- information about patients is recorded clearly and accurately, so that it can be easily read and relied upon by others providing care

Information governance also covers the effective management of employee data and corporate business information required for service planning and performance management.

| ***Information means:*** | ***Handling information means:*** |
|---|---|
| **Personal data** e.g. name, date of birth, home address, NHS number, hospital number etc.<br><br>**Sensitive data** e.g. religious beliefs, ethnic origin, criminal record, medical records etc.<br><br>**Corporate data** e.g. Trust accounts; statistical reports; contracts; minutes of meetings etc. | **H**olding it **securely** and **confidentially**<br><br>**O**btaining it **fairly** and **efficiently**<br><br>**R**ecording it **accurately** and **reliably**<br><br>**U**sing it **effectively** and **ethically**<br><br>**S**haring it **appropriately** and **lawfully** |
| ***Formats covered:*** | Paper, electronic, audio, video, x-rays, email, text etc. |

The Trust is bound by the provisions of a number of items of legislation affecting the stewardship and control of information.

## *Key legislation and standards*

**Data Protection Act 1998** - governs how personal data belonging to living individuals is processed, including how information is obtained, held, used and disclosed

**Freedom of Information Act 2000** - sets rules for disclosure of non-personal information about the work carried out by public sector organisations

**Computer Misuse Act 1990** - relates to electronic records in that it creates three offences of unlawfully gaining access to computer programs and data

**Common law duty of confidentiality** - 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.

**Professional Codes of Conduct** - all NHS professions have their own codes of conduct setting out the standards of ethical behaviour owed by members of each profession. These standards include respecting patients decisions about their care and treatment; obtaining consent for treatment or for disclosure of patient personal information; protecting patient personal information by maintaining confidentiality and ensuring continuity of care through good record keeping practice.

**NHS Confidentiality Code of Practice** - explains how to provide a confidential service to patients and how to comply with the common law duty of confidentiality

**NHS Records Management Code of Practice** - provides guidance on the management of **all** types of NHS records, patients, staff and corporate, throughout their lifecycle *(creation → use → retention/storage → appraisal → disposal)* and details the minimum retention periods.

**NHS Information Security Code of Practice and Information Security Standards – ISO/IEC 17799: 2005** - sets out how organisations should comply with information security principles and includes some mandated actions such as encryption

**NHS Care Record Guarantee for England** - tells patients how their information will be used by NHS organisations so that their rights are protected and their health & wellbeing promoted

**Information Quality Assurance** - guidance to support the effective use of data standards across the NHS

## Why you need to know about information governance

Everyone who works in health or social care must be aware of the following:

- How important the information we hold is
- What legislation, guidelines and best practice there is for looking after such important information
- Why you must take responsibility for how you obtain, record, use, keep and share information

All staff (permanent, temporary or contracted) are personally responsible for ensuring that they are aware of the information governance requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Managers are also responsible for promoting information governance standards and ensuring compliance by the team members.

### *Contracts of employment*

All NHS staff members have a legal duty of confidence to patients and are required to meet the standards set out in their terms of employment.

All Trust staff have a duty to keep all information about patients, staff or Trust business confidential.

Failure to meet the standards set out in the confidentiality and access to information clause of Trust employment contracts can result in disciplinary action, termination of a contract, dismissal and in some cases criminal charges.

For example, disciplinary action could follow:

- Unauthorised disclosure of information
- Deliberately looking at records without authority
- Discussion of personal information in an inappropriate venue
- Transferring personal information electronically without encryption etc.

Under data protection legislation unlawful access and disclosure of confidential data can lead to prosecution and an unlimited fine.

You must not:

- access records without authority
- divulge information relating to patients, staff or the Trust to anyone other than authorised persons
- remove records or information from the Trust's premises and control without the approval of senior management
- discuss personal details in a non-working capacity or transfer personal information electronically without proper permission and encryption

You should comply with the requirements of the Data Protection Act and act in accordance with the guidelines detailed in the Trust's policies and procedures, including the **Information Disclosure Policy** and the **Code of Conduct for Handling Personal Identifiable Information**.

Ensure that the information is kept secure and that the information you record is accurate, factual, reliable and fit for purpose.

ALL PERSONAL INFORMATION MUST BE TREATED WITH CARE AND KEPT CONFIDENTIAL

INFORMATION GOVERNANCE IS **EVERYONE'S** RESPONSIBILITY

## *Your responsibilities*

- Keep data secure and follow security procedures (safe haven, encryption)
- Record accurate information
- Be aware of the Data Protection and Caldicott Principles
- Use & share information appropriately and lawfully
- Respect the rights of individuals and comply with access to information requirements
- Report suspected or actual incidents or concerns
- Familiarise yourself with Trust IG & ISMS policies … if in any doubt, contact the IG team before taking any action

## *Where to go for more guidance*

1. LHCH Information Governance policies:

   Code of Conduct for Handling Personal Identifiable information
   Corporate Records Management Policy
   Data Quality policy
   Health Records and Case Note Management policy
   Information Disclosure policy
   Information Governance policy
   Information Risk policy

2. LHCH Information Security Management System:

| **To be read by all staff** | **To be read by Information Asset Owners, IT staff and project managers** |
|---|---|
| Standard 1. IG and safe haven | Standard 2. Security control of assets |
| Standard 3. Access control to secure areas | Standard 6. System planning, procurement and acceptance |
| Standard 4. Equipment security | Standard 8. Housekeeping |
| Standard 5. Computer and network operations | Standard 9. Data and software exchange |
| Standard 7. Protection from malicious software | Standard 12. Computer access control |
| Standard 10. Monitoring system access and use | Standard 13. Application access control |
| Standard 11. User access control – password policy | Standard 14. Data validation |
| Standard 16. Security incident management | Standard 15. Security of application systems |
| Standard 17. Forensic readiness | Standard 18. Risk assessment |
| | Standard 19. Business continuity planning |

3. NHS Code of Practices / Department of Health publications:

   - Confidentiality
   - Records Management Part 1
   - Records Management Part 2
   - Information Security
   - NHS Information Governance Guidance on Legal and Professional Obligations

4. Visit the Information Governance intranet site

5. Information and guidance is also available on the following websites:

    - Information Commissioner's Office
    - Health and Social Care Information Centre
    - Department of Health

6. Contact the IG Team:
    - **Liam McCormack, Information Governance Facilitator**
      0151 600 1845 Liam.McCormack@lhch.nhs.uk
    - **Carol Taylor, Information Governance Officer**,
      0151 600 1240 Carol.Taylor@lhch.nhs.uk
    - **Wyn Taylor, Information Governance & Health Records Manager**,
      0151 600 1368 Wyn.Taylor@lhch.nhs.uk
    - **Paul Leddy, Health Records Co-ordinator**
      0151 600 1978 Paul.Leddy@lhch.nhs.uk
    - **Gemma Owen, IT Security Officer**
      0151 600 1525 Gemma.Owens@lhch.nhs.uk
    - **Dr Raph Perry, Caldicott Guardian**,
      0151 600 1429 Raphael.Perry@lhch.nhs.uk
    - **Dr Mark Jackson, Senior Information Risk Owner**
      0151 600 1332 Mark.Jackson@lhch.nhs.uk

# Confidentiality

All NHS employees have a legal duty of confidence to protect the information that becomes known to them during the excise of their duties and have a personal responsibility to comply with relevant legislation and related Trust policies.

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.

Confidentiality is a legal obligation that is derived from case law, known as the common law duty of confidentiality, and is a requirement established within professional codes of conduct and NHS employment contracts.

Failure to meet the standards set out in the Confidentiality clause of Trust employment contracts can result in disciplinary action, termination of a contract, dismissal and in some cases criminal charges.

Managers must ensure that their staff are aware of and understand their obligations to conform to standards of confidentiality, outlined in the Trust's **Code of Conduct for Handling Personal Identifiable Information** and the **Confidentiality NHS Code of Practice**. They are also responsible for ensuring their staff are notified of any changes.

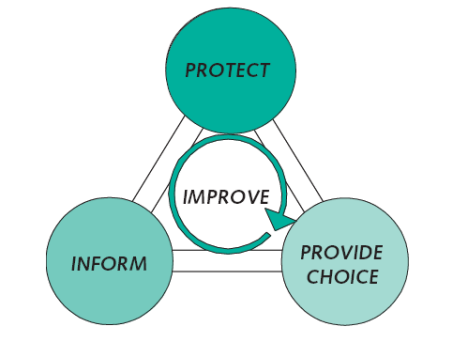
All staff including contractors, volunteers and non-executive directors are obliged to adhere to this code of conduct.

**A failure to adhere to the NHS Confidentiality Code of Conduct and associated Trust policies and procedures may result in disciplinary action.**

## *The Confidentiality Model*

The model outlines the requirements that must be met to provide patients with a confidential service:

**PROTECT** – patient information must be kept private and physically secure, and used & disclosed with appropriate care




**INFORM** – patients must be made aware that the information they provide may be recorded and shared to provide them with care. The Trust's website and 'In Confidence - Protecting Your Privacy' leaflet are available for patients.

**PROVIDE CHOICE** – patients must be allowed to decide whether their information can be used or disclosed in ways that ***do not*** directly contribute to or support the delivery of care.

Patients **must** give explicit consent for **all non-healthcare uses of their data** e.g. disclosures outside the Trust to non-healthcare organisations or for medical research.

**IMPROVE** – all data security breaches, near misses or risk of breaches must be reported and you should seek training or support if uncertain of how to handle confidential information.

## The Caldicott Review

The review was commissioned by the Chief Medical Officer of England owing to increasing concern about the ways in which patient information is used in the NHS in England and Wales and the need to ensure that confidentiality is not undermined.

Such concern was largely due to the development of information technology and its capacity to disseminate information about patients rapidly and extensively.

The 1997 report of the Review of Patient Identifiable Information, chaired by Dame Fiona Caldicott (the Caldicott Report), made a number of recommendations for regulating the use and transfer of patient identifiable information between NHS organisations in England and to non-NHS organisations.

The review covered all patient identifiable information for purposes other than direct patient care, medical research or where there was a statutory requirement for information. The aim was to ensure that information was only shared and used for justifiable purposes and that only the minimum necessary information was shared. The review also provided guidance on actions to minimise confidentiality risks.

The recommendations of the Caldicott Review Committee have come to define the NHS confidentiality agenda. Confidentiality is an essential component in the provision of health care and clinical professions have stringent requirements with regards to confidentiality in their codes of practice.

Central to the recommendations was the appointment of a 'Guardian' of person-based clinical information, responsible for overseeing the arrangements for the use and sharing of clinical information.

The Trust's Caldicott Guardian is Dr Raph Perry, Consultant Cardiologist and Medical Director - Raphael.Perry@lhch.nhs.uk - 0151 600 1429

Another key recommendation of the review was that every use or flow of patient-identifiable information should be regularly justified and routinely tested against the Caldicott Principles. To comply with this all Departments are required to identify, map and risk assess all routine transfers of person-identifiable and confidential information annually.

### Caldicott Review Two – Information to Share or Not to Share? The Information Governance Review March 2013

Following a request from the Secretary of State for Health, Dame Fiona Caldicott carried out this independent review of information sharing to ensure that there is an appropriate balance between the protection of patient information and the use and sharing of information to improve patient care. A total of

26 recommendations were made by the Review Panel including the need to update existing principles and the introduction of an additional principle.

### *The Caldicott Principles*

| Principle: | Guidance: |
|---|---|
| 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 | Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out. |
| 4. Access to personal confidential data should be on strict need to know basis | 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. |
| 5. Everyone with access to personal confidential data should be aware of their responsibilities | 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. |
| 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. |

## NHS Care Record Guarantee for England

The NHS Care Record Guarantee sets out the rules that govern how patient information is used in the NHS and what control the patient can have over this. It is based on professional guidelines, best practice and the law and applies to both paper and electronic records.

The **NHS Care Record Guarantee** includes information on:

- people's right of access to their own records
- how access to an individual's healthcare record will be monitored and policed and what controls are in place to prevent unauthorised access
- options people have to further limit access
- access in an emergency
- what happens when someone is unable to make decisions for themselves

The delivery of joined up care requires effective and accurate sharing of information between health and social care. The NHS Care Record Guarantee for England and the Social Care Record Guarantee for England together form a basis for transparent, legal and secure information sharing.

The guarantee was first published in 2005 and is regularly reviewed by the National Information Governance Board to ensure it remains clear and continues to reflect the law, professional guidelines and best information governance practice. It was last published in January 2011.

# Data Protection Act 1998

All NHS organisations must comply with the Data Protection Act (DPA) 1998 which governs the processing of information held by organisations that can identify a living person (the data subject). The Act came into force on 1 March 2000 and requires that organisations (or data controllers) collect and process personal data fairly and lawfully, in line with the Data Protection Principles.

Personal information is defined as any information that enables the identification of a living individual. The information can be complete or be pieces of information in the possession of the data controller that when taken together can lead to the identification of a person.

Personal data is information that is processed electronically and held manually, and there are two categories:

- **Personal data** includes name; address; date of birth; NHS number etc. Some personal information is defined as sensitive personal data and even more stringent measures must be taken to ensure that sensitive data remains secure.

- **Sensitive information** includes religious beliefs; ethnic origins; health or physical condition; trade union membership; political views; sexual orientations; criminal convictions.

## *The Eight Data Protection Principles*

Personal data shall be:

| | |
|---|---|
| 1. | **Processed fairly and lawfully**<br>• Be open, honest and clear with people (patients and staff), tell them why their information is being collected, how it will be used and who it may be shared with and why<br>• Provide patients with information leaflets if applicable |
| 2. | **Processed for limited purposes**<br>• Understand why personal information is being used or requested<br>• Only use personal information for the purpose for which it was obtained<br>• Only share personal information outside your Department or the Trust if you are certain it is appropriate and necessary to do so<br>• If in doubt check first with your line manager or the IG Team |
| 3. | **Adequate, relevant and not excessive**<br>• Only collect and record the information your require for the current purpose<br>• Stick to the facts and avoid personal opinions and comments<br>• Use clear legible writing and explain all abbreviations |
| 4. | **Accurate and up to date**<br>• Take care when recording or inputting information<br>• Check that data is up to date, ask patients to confirm their details (address; date of birth, telephone number etc.)<br>• Check existing records thoroughly before creating new records to avoid duplicated records |
| 5. | **Not kept longer than necessary**<br>• Don't hold information 'just in case it might be useful one day'<br>• Follow record retention guidelines and review data regularly<br>• Remember the Records Management: NHS Code of Practice<br>• Dispose of information securely |
| 6. | **Processed in line with the data subject's rights**<br>• Individuals rights under the Act: |

| | |
|---|---|
| | ○ to access a copy of their information<br>○ to object to processing that is likely to cause or is causing damage or distress<br>○ to prevent processing for direct marketing<br>○ to object to decisions being taken by automated means<br>○ in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed<br>○ to claim compensation for damages caused by a breach of the Act |
| 7. | **Secure**<br>• Take practical steps to protect data for example follow safe haven procedures; operate a clear desk policy, use secure transfer methods e.g. email encryption<br>• Follow Trust policy and procedures for handling and disclosing personal information e.g. Code of Conduct for Handling Personal Identifiable Information |
| 8. | **Not be transferred to other countries without adequate protection**<br>• Don't transfer information without consent or without ensuring that the data is adequately protected<br>• Check where information is going before releasing it<br>• Obtain approval from the Caldicott Guardian, Dr Raph Perry or Information Governance & Health Records Manager (Data Protection Officer), Wyn Taylor |

### *Subject Access Requests*

The Data Protection Act allows certain rights to data subjects (the person whose data has been collected) and the most common request in the NHS is the right of subject access, the right to know what personal information is on a computer or in manual records held by the organisation. More often than not this is a request to view or have a copy of their medical record. The right can also be exercised by an authorised representative on the individual's behalf e.g. solicitor.

All staff should know the details of the appropriate person who deals with these requests, as they must be dealt with in a specific manner. To comply with the Act the organisation has 40-calendar days from the receipt of the request, to verify the identity of the applicant, locate the relevant information and to provide access to it. LHCH does not routinely charge for processing subject access requests.

If however there is potential disproportionate effort to comply with a request or to provide in a specifically requested format other than the Trust's usual process, then a charge may be applied

Requests for access to personal information or health records are co-ordinated by the Information Governance Team, with the exception of requests relating to legal claims which are dealt with by the Trust's Legal Services. Requests should be made in writing and application forms are available on the intranet or from Health Records - Phone: 0151 600 1240 | Email: infogov@lhch.nhs.uk.

Requests must be date stamped and forwarded immediately on the same working day to Information Governance, Health Records Department, 3rd Floor, Liverpool Heart and Chest Hospital NHS Foundation Trust, Thomas Drive, Liverpool, L14 3PE.

More information on disclosing of information can be found in the **Information Disclosure policy**.

## Freedom of Information Act 2000

The Act came fully into force from the 1 January 2005 and gives the general right to anyone to access official information held by public authorities.

Requests must be made in writing (email is acceptable) and state what information is required. The applicant does not have to state the request is a Freedom of Information request and they do not have to state why they want the information.

Requests can be for any information held by the Trust, anything that substantiates how decisions were made and by whom, how monies were spent or apportioned and can include; hand written notes; PowerPoint presentations; word documents (such as minutes / reports / consultation documents / letters); emails; spread-sheets; photos & images.

The release of corporate information held by the Trust is coordinated centrally; if you receive a request it should be forwarded immediately to Information Governance - email to FOIRequests@lhch.nhs.uk or post to Freedom of Information, Health Records Department, 3rd Floor, Liverpool Heart and Chest Hospital NHS Foundation Trust, Thomas Drive, Liverpool, L14 3PE.

Information Governance will then log the request and approach the appropriate department to provide the relevant information. There are a number of designated department leads in the Trust who are responsible for providing information in a timely manner to ensure that the request is processed within the legal timeframe.

If you're asked to provide information for a request you must respond as quickly as possible. All requests have to be dealt with within 20-working days. FOI requests are not for personal information; personal data can only be released in compliance with the Data Protection Act. See Data Protection section.

The Act also requires every public authority and organisation that receives government funding to maintain an approved Publication Scheme, which is a means of providing access to information which the organisation proactively publishes such as annual reports; Board minutes etc. Any fees charged for providing information requested under FOI will be displayed on the Publication Scheme. The Trust's Publication Scheme can be found on the Trust's website - www.lhch.nhs.uk

## The Information Commissioner

It is the Information Commissioner's function to uphold the information rights of individuals and to ensure compliance with the Freedom of Information Act, the Data Protection Act and the Environmental Regulations (covers requests for corporate information relating to the environment). The Information Commissioner's Office has the power to issue undertakings or enforcement notices and to impose financial penalties of up to £500,000 for serious data breaches and if needs be to initiate court proceedings to ensure compliance.

The Acts and regulations support each other allowing public access to information held by the public sector. Destroying requested information outside of normal Trust policies is unlawful and may be a criminal offence if done to prevent disclosure.

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF | Helpline Tel: 08456 306060 or 01625 545745 Monday to Friday 9am to 5pm | Fax: 01625 524510 | Press and media enquiries Tel: 020 7025 7580 | www.ico.org.uk

## Record keeping and data quality

Good quality information is critical for:

- Patient Care
- Minimising clinical risk
- Effective and efficient clinical and administrative processes, such as communication with patients and their representatives
- Payment by Results – Trust income determined by services and treatment provided
- Management decision making as well as strategic planning
- Performance reporting to stakeholder and commissioner groups
- The establishment of acceptable service level agreements and contracts
- Clinical governance
- Safeguarding of both adults and children
- Effective health protection
- Benchmarking – both internal and external
- Identification of appropriate healthcare target populations

### *Data quality criteria*

| | |
|---|---|
| Complete | Captured in full, with no missing items and includes the patient's NHS Number |
| Accurate | No errors |
| Relevant | Appropriate for the use to which it will be put |
| Accessible | Readily available when required … track all case note movement on ICS |
| Timely | Records should be written contemporaneously i.e. at the time an event occurred |
| Free from duplication | Before creating a new record make sure that one doesn't already exist |
| Defined | Fully explained and agreed by all stakeholders and where necessary in appropriate documentation |
| Appropriately stored | Stored securely (paper & electronic data) and protected from inappropriate access |
| Appropriately sought | Collected only once per episode rather that repeatedly gathered and should be gathered using the most appropriate method |

Further guidance is available in the Data Quality staff information leaflet and from the Data Quality Team – Email DataQualityTeam@lhch.nhs.uk or Phone 0151 600 1553.

A high standard of clinical record keeping is fundamental to the delivery of safe and effective care and the Trust's **Clinical Record Keeping** policy outlines the standards expected and includes details of the areas identified for audit.

# Records Management

Records Management is an essential element of Information Governance and effective records management aims to ensure that information is properly managed and is available whenever and wherever there is a justified need for that information.

In the case of personal information, it is also a legal requirement. You must feel confident that you know how to access and store information in a consistent manner to enable you to perform your job to the best of your ability. Laws that apply to the handling and use of health records are:-

| | |
|---|---|
| Public Records Act 1958 | Data Protection Act 1998 |
| Access to Health Records 1990 | Common Law Duty of Confidentiality |
| Computer Misuse Act 1990 | Code of Practice on the management of records – Section 46 of the FOI Act |

Further guidance can be obtained on the **Information Governance** intranet site and in the Department of Health's Records Management: NHS Code of Practice

- **Records Management Part 1**
- **Records Management Part 2 (Retention and destruction schedules)**

Remember everyone working in healthcare, who records, handles, stores or deals with information has a personal common law duty of confidentiality.

## *Manual Records*

Manual records (paper based) should be stored securely when not in use and confidential information such as patient health records or employee records must not be where they may be viewed by members of the public or unauthorised staff.

Records must not be taken offsite **without prior** approval.

Although the Trust uses the Electronic Patient Record (EPR) to record all assessments, treatments, procedures and medications given to patients there are also a number of paper based documents in use.

Refer to the Trust's **Health Record and Case Note Management Policy** for further guidance.

## *Electronic Records*

- Access to any PC or computerised system must be password protected.
- Passwords must not be shared.
- Access to personal and confidential information must be restricted to staff who require access using appropriate access permissions supported by access control (user name and password)
- EPR access is on a **legitimate relationship** basis
- Computer screens must not be left on view so members of the public or staff who do not have a justified need to view the information can see personal data
- When not in use, PCs and laptops should be switched off or have a secure screen saver activated … press the **Windows key and L** or **CTRL – ALT – DEL keys and enter**
- Laptops should be kept secure and be protected by encryption software (Safeboot)
- Records **must not** be saved to local C:\ or personal H:\ drives. Records must be stored in network drive folders (e.g. W:\, K:\ etc.), which provided security and routine back-up of data
- Unencrypted portable media such as USB data sticks must not be used for confidential information
- Dormant or inactive electronic records should be archived on the network drive and be retained for the appropriate retention period

## *Electronic Patient Record (EPR)*

EPR was introduced on 26 June 2013 providing greater access to patient data. In line with the duty and commitment of the NHS to keep patient information safe, secure and confidential, patient records **must only** be accessed where a legitimate relationship exists. The system is fully auditable and any inappropriate access identified will be investigated and could lead to disciplinary action being taken including dismissal.

### Legitimate relationship

The EPR record has been accessed by a registered and regulated health professional who is involved in the direct care of the patient.

A legitimate relationship with the patient will be when the EPR record has been accessed by a registered and regulated health professional who is involved in the direct care of the patient and when any or all of the following criteria are met:

- The individual presents themselves to the professional to receive care
- The individual agrees to a referral from one care professional to another
- The individual is invited by a professional to take part in a screening programme for which they are eligible and they accept
- The individual presents to a health or social care professional in an emergency situation where consent is not possible
- The relationship is part of a legal duty
- The individual is told of a proposed communication and does not object e.g. Consultant states they will contact another professional for opinion and the patient does not object

Non-clinical members of staff **must only** access the EPR where they have a legitimate business reason to access the patient's clinical information as part of their job role for example members of the clinical audit team.

## *Electronic Document Management System (EDMS)*

The EDMS tab within allows the scanned images of paper health record documents to be viewed. The Scanning Bureau located in the Health Record Department is responsible for scanning the majority of records although some documents are sent automatically into EDMS by other systems (e.g. Excelera Cardiology reports) and some are scanned by Wards.

All documents received by the Bureau are scanned within 24 hours of receipt; to ensure that EPR records are as up to date as possible the following actions are essential:

- A barcoded label must be attached to the first page of each individual document generated during a visit. These labels contain the patient MPI number and unique visit ID (eight digits for inpatient stays and 12 digits for outpatient appointments) and ensure that scanned documents go straight into the EPR record
    - Care must be taken not to use other labels instead of the barcoded label such as blood labels or labels without the unique visit ID
- Documents must be filed into the temporary case note folder created for the patient's visit, inpatient (purple) or outpatients (orange)
- Inpatient and outpatient case note folders must be available for scanning immediately after the end of the visit
    - folders must not contain documents for more than one patient
    - folders must not be taken away from clinic

For documents scanned outside the Bureau it is essential that they also contain the barcoded label, without a label the document will not be indexed or appear in the patient EPR record.

### *Retention and Destruction of Records*

NHS records containing personal information must not be kept longer than necessary, and corporate business records must be retained for the minimum period of time for legal, operational, research and safety reasons.

The length of time for retaining records will depend on the type of record and its importance to the Trust's business functions. Guidance is given in the Department of Health **Records Management: NHS Code of Practice Part 2 (Retention and Disposal Schedules)**.

If your specific record type is not detailed within the national retention schedule please contact Information Governance (**infogov@lhch.nhs.uk** | 0151 600 1240 /1845) for guidance.

The disposal / destruction of personal and confidential records must be carried out securely, guidance on the Trust's procedures can be found on the **Information Governance** intranet site.

## Information Security

All records containing personal information whether they are kept in paper files or stored on PCs, laptops or any other form of electronic capture device must be secure.

The Trust's **Information Security Management System (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.

The ISMS provides guidance to all users of Trust information and information systems of their responsibilities and the required security standards to be followed.

The ISMS policy and procedure documents are available on the intranet but some basic rules for maintaining the confidentiality of personal information are detailed below:

### Accessing data for personal reasons (inappropriate access)

- Confidential data must **only** be accessed by employees where they need to access that data as part of their job i.e. where a legitimate relationship exists
- It is illegal to access data for personal reasons, for example you must not look up results of family members or friends, or access your own information unless authorised to do so or where a legitimate relationship exists

## Giving information to other people (disclosing patient information)

- Personal information given in confidence should not be disclosed further or used for another purpose unless:
    - The individual has given their explicit consent
    - The disclosure is a requirement of a statue of law
    - There is an overriding public interest in making the disclosure
- When collecting information from patients they should be made aware how their information will be used & shared, and their consent obtained. They should understand information disclosures that must take place in order to provide them with high quality care.
    - Details about how LHCH processes information can be found on our website or in the In Confidence: Protecting your privacy patient information leaflet
    - Queries regarding use of information should be passed to Information Governance or PALS (our Patient and Family Support Team)
- Explicit consent is required for:
    - Disclosure outside the Trust to non-healthcare organisations e.g. housing departments, the police, voluntary services etc.
    - Sharing and use for non-care purposes such as research, public health surveillance, checking the quality of care and managing care services
- You **must not** disclose any information to outside agencies or organisations unless it is appropriate to do so. For example, with the consent of the individual; in line with an existing information sharing agreement or if patient consent is not held approval from our Caldicott Guardian.
- Patient information must only be shared on a 'need to know' basis with other NHS organisations. All requests for such information should be in writing, on headed notepaper; via fax or NHS email. You must only return the data requested to a secure environment e.g. via encrypted email or faxed to a registered Safe Haven fax machine.

Further guidance on disclosing patient information can be found on the **Information Governance** intranet site or can be obtained from the Information Governance team or the Trust's Caldicott Guardian.

## Information Sharing Agreements

The sharing of information plays a key role in providing high quality care and information sharing is central to the Government's goal of delivering better more efficient public services.

It may be necessary for essential personal information to be shared between NHS organisations and with external non-NHS organisations such as local authority social services. Where confidential personal information that can identify individuals is being shared routinely or in bulk (relating to 51 or more individuals) then an Information Sharing Agreement (ISA) should be set up, this is particularly relevant if the sharing is for a non-care purpose.

ISAs are operational documents which outline the principles and rules that will be followed, consent procedures, legal compliance, security requirements etc. ISAs provide staff with details of what data is to be shared and how and when the data will be shared. You must follow agreed ISAs if they are in place.

## Safe Havens

The term 'Safe Haven' originally referred to the siting of fax machines, however the meaning has since been expanded to encompass all secure points at which confidential information is received. The Trust must ensure that there are procedures in place to ensure that personal information is received into secure and protected points. All points of receipt should be considered including:

- Transcribing of phone messages
- Fax machines
- Electronic mailboxes
- Pigeon holes and post in-trays for paper information

Each department should have at least one designated safe haven contact point. Ideally, all information transmitted to the Trust should pass to these contact points and safe haven procedures should cover all flows of person identifiable information.

## Faxing

- Fax machines must be secure and located in non-public areas
- Do not fax personal or confidential information unless it is absolutely necessary
- You must establish that there is a justified reason to share the information
- Release information on a 'need to know basis', send the minimum amount of personal information only and wherever possible send anonymised or depersonalised information

- Send the information to a secure safe haven fax or contact the recipient before transmission to ensure that they are waiting to receive it if sending to an unsecure fax
- Check the fax number before sending
- Use a fax header cover sheet with a disclaimer giving details of who to contact if received in error
- Faxes containing confidential sensitive information should be sent to a named individual, clearly marked 'Private and Confidential'
- Ask for confirmation of receipt
- Retain the transmission confirmation after checking to ensure that recipient's details are correct and that the fax was sent successfully
- Programme regularly used numbers into the fax machine where possible

## Email

- Personal information that identifies a patient or member of staff or commercially sensitive business information **must not** be sent outside of the Trust by email unless it is encrypted to NHS standards.
- Email must only be used to transfer person-identifiable information where it is absolutely necessary to do so.
- Emails containing personal or confidentiality information must be sent using one of the approved methods:
  - Between internally managed Trust email accounts (@lhch.nhs.uk to @lhch.nhs.uk) providing that the message is sent from and to an appropriate NHS sited computer
  - Using the Trust encrypted email solution (Safend)
  - Using NHSmail (@nhs.net to @nhs.net), providing that checks are made to ensure that the recipient also has an NHSmail account and that the message is sent from and to an appropriate NHS sited computer

## Telephone

- Phone calls to discuss sensitive information should take place in a private location
- Recording and replaying voice mail messages should be done in a private location
- **Before** disclosing sensitive information
  - Always check who you are speaking to, includes patients, carers, members of staff or third parties
  - Confirm the reason for the request
  - Obtain a contact number and advise that we will call them back. This **must** the main switchboard number, not a mobile or direct dial number
  - Where possible, request a written request (can be sent by email or fax)
  - Check that the information can be released (is the reason for the request valid and justified?)
  - Confirmation that a patient has attended a clinic or surgery session should not be disclosed without permission from the patient
  - Provide the information only to the requestor on a 'need to know' basis (the information should be relevant and not excessive), using a validated phone number, do not leave a message
  - Make a record of the disclosure including the reason, who requested the information (name, job title, organisation, telephone number), date & time, who authorised release and your name & job title

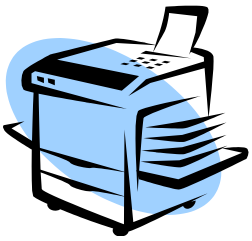
**If in doubt, please contact your manager, our Caldicott Guardian or Information Governance**

## Post

Only send patient-identifiable information where it is absolutely necessary to do so and then only send the minimum amount of information necessary.

- Confirm the name, department and address of the recipient
- Dispatch using strong envelopes that are sealed securely. Bulky material should be sent using strong boxes or containers again sealed securely
- Clearly address the envelope with the recipient's name and address. Information being sent to a team should be addressed to an agreed post holder or the team leader
- Clearly mark the envelope '**Private and Confidential**' or for highly sensitive information mark as '**Strictly Private and Confidential - to be opened by addressee only**'
- Take care when using envelopes address windows to make sure that no other information is visible through the window
- Copies rather than originals should be sent, wherever possible
- Confirmation of receipt should be obtained, where deemed necessary following local risk assessment
- Transfers of complete records (original or copy) or data relating to more than 51 individuals i.e. bulk transfers outside the Trust:
    - must be sent using 'track & trace' mail e.g. recorded delivery, Trust approved courier
    - confirmation of receipt must be obtained
    - double-envelope for extra security
- Post collection and delivery points should be in secure areas
- Unsecured post collection points should be emptied at the end of each day, uncollected mail should be locked away until the next day or hand delivered to the mailroom for despatch
- Incoming post should be opened away from public areas, correspondence should be should be placed faced down and not be left unattended
- Post should be handed to the relevant member of staff for action, not left unattended on their workstations. If the named recipient is unavailable store the post securely until they return

## Photocopying



- Only copy if you really need to and keep the number of copies to a minimum
- Take care when sending on copied or printed confidential data, check it's going to the right recipient
- Regularly check and update your distribution list to ensure copies are not sent to staff who have left or moved to another service

## Smartcards

Your Smartcard provides you with the level of access to healthcare information you require as part of your healthcare role. It is your responsibility to ensure the safety of your Smartcard and patient data. You must read, understand and sign the declaration on the RA01 form to agree your responsibilities to always keep your smartcard safe and use it appropriately in line with the following user responsibilities:

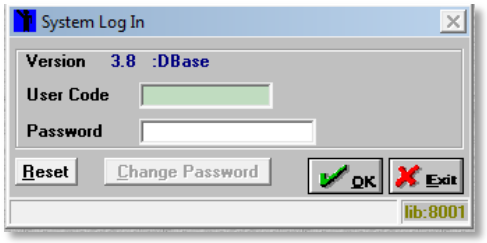

- You have a duty to keep patients data secure and confidential
- Keep your Smartcard safe at all times and ensure that it is used appropriately
- Keep your Smartcard safe and separate from its PIN number when not in use
- Never tell anyone your PIN number
- Never allow anyone else to use your Smartcard
- Do not write your PIN number down anywhere
- Never leave your Smartcard in the Smartcard reader when you are not actively using it
- Access through clinical systems to patient identifiable information is on a

need to know basis and accessing records unless the user has a legitimate reason will be viewed as a breach of confidentiality and may lead to disciplinary action

- Report the loss, theft or damage of your Smartcard immediately directly to your Manager and then log a call with the IT Service Desk. The Service Desk will contact the local Registration Authority so they can cancel your card and replace it as soon as possible. Complete and submit an incident report, using the Trust incident form or on the **online incident reporting system**.

## Passwords

Passwords help us to maintain the confidentiality of records and to comply with the legal requirement to protect personal data with adequate security.




- Choose a different password for each system or account you access … one password is easy to remember, but it's also easier to break and increases the risk of information getting into the wrong hands
- Choose a secure password, one that's hard to guess
  - a combination of letters, numbers and symbols
  - a mixture of 'UPPER' and 'lower' case characters
  - something memorable but not too obvious
  - a minimum of six characters
- Never write your password down, if you need a memory jogger, write down a trigger word, not the password itself
- Keep prompts / reminders in a secure place
- Never let others see you enter your password
- Change your password regularly
- Never share your password or allow others to use your access.
  If you believe some else may know your password contact the IT Service Desk immediately on 0151 600 5499 asking for your password to be reset

## Computer

- Never leave your screen displaying sensitive information or unlocked so that others could use it to access or view sensitive information. Always lock your workstation, do this by pressing these keys:
  - *Windows key and L*
  - *CTRL – ALT – DEL keys together then ENTER*
- Position your computer screen so that confidential information cannot be seen by visitors or unauthorised staff
- Keep your password confidential
  - don't write it down
  - never divulge your username and/or password to anyone else
  - change your password regularly
- Never use someone else's username or password to log on to your computer system.
  A computerised audit trail is kept of user access and failure to comply with this is a disciplinary offence.
- Store personal and confidential information on the Trust's shared network **never** store it on:
  - the computer's local hard-drive (C:\ drive)
  - unencrypted portable media such as USB data sticks
- Don't install unauthorised software
- Log off your computer when leaving the office

## Transporting personal identifiable information including case notes

- Medical records should be transported in sealed bags or face down in trolleys (lockable trolleys if available)
- Trolleys must not be left unattended in public areas
- Loose papers must be carried securely
- Confidential information must be carried in lockable bags or sealed envelopes and must not be left unattended

- Prior approval is required before case notes can be taken offsite and must be returned the same day. In exceptional circumstances **only** where this is not possible, authorisation must be obtained and steps taken to secure the information overnight
- Information transported by car must be not be visible and should be stored in the locked car boot. No information must be left in a car or car boot overnight

## Portable/removable information media and

(Laptops, tablets, iPhones, Blueberry, mobile/IP phones, USB data sticks, CDs, DVDs, SD or PDA memory cards etc.)

- Confidential personal identifiable information and business sensitive information **must not** be transferred:
  - to unsecured portable media
  - to portable media unless it is part of an authorised Trust data flow and is encrypted to the required NHS standards (Trust approved encrypted USB data sticks are available for use – **online application form**)
- All Trust computer and laptop USB ports are secured with Safend, a software solution to prevent the use of unsecure media
- Laptops and other media should be locked away when not in use
- Devices must be transported discretely and securely
- Don't use removable media for any purposes you wouldn't use them in work
- Never let anyone else use Trust equipment
- Turn off Bluetooth and wireless access if not in use
- Don't connect several network interfaces at once or attempt to share the connection

## Remote access / occasional home working

- Remote/home working using IT equipment is only permitted for authorised staff (applications for remove access should be submitted to the IT Team)
- Managerial authorisation is required for remote working using paper records
- Be aware of the environment you're in and don't look at confidential information where it can be seen by someone else
- Follow the key standards set out in **ISMS security standard 1**

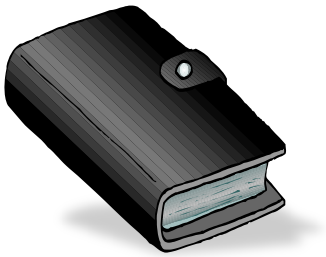
## Bins

- Make sure that you dispose of confidential information appropriately
- All personal information is confidential and must be shredded or placed into confidential waste bins. Never place into general waste bins.
- Confidential waster paper must not be used as scrap paper for messages; notes etc.

## Your work environment

- Remember to wear your identity badge at all times
- Whenever possible escort visitors at all times on site
- Operate a clear desk policy, especially if hot-desking or working in an open plan office.
- All confidential information must be placed out of sight, in locked cabinets/drawers when not in use
- Ensure that filing cabinets containing confidential information are kept locked when not in immediate use and are sited in areas that are not accessible to members of the public or visitors
- Carry out regular housekeeping of your files, destroy information in line with NHS retention guidelines and Trust procedures
- Lock and secure your office when it is unattended and at the end of the day, all windows and keypad doors closed
- Carry out end of day checks to ensure that all confidential information is locked away securely. Check there are no faxes left on the fax machine; print outs left on the printer or any confidential data on notice boards / dry-wipe boards

## Diaries (clinical appointment)



- Diaries must only contain the minimal information necessary for staff to undertake their role:
    - Names and addresses for visits … where ever possible use initials instead of full names
    - No identifiable medical or treatment information against the patient's name
    - No identifiable key codes against a patient's name
    - No phone numbers against the patient's name
- Do not keep other documents in diaries e.g. prescription pads
- User names and passwords to NHS systems must not be written down
- Transport securely, out of sight in locked car boot
- Keep secure when not in use e.g. stored in a locked drawer in the office base
- Diaries must be kept for a minimum period of 2-years after the end of the year to which diary relates
- Patient specific information should not be recorded in diaries however such must be transferred to the patient's record as soon as possible.
    - Diaries must be destroyed under confidential conditions at the end of the 2-year retention period in line with Trust policy and procedures.

## Person

- Ensure you hold confidential conversations in an appropriate place, do not discuss confidential information in corridors; open plan offices or at the photocopier
- Wherever possible gain the patient's consent before sharing their personal information including with relatives

## Privacy Impact Assessments (PIA)

The introduction of new systems and services or changes to existing ways of working can have a major impact on the Trusts ability to maintain the confidentiality, integrity and accessibility of personal information, in both paper and electronic formats.

Before any changes are made or new processes are introduced, the Trust must ensure that potential risks to privacy are identified and steps taken to mitigate them, ensuring compliance with IG legal requirements.

The Trust's PIA screening pro-forma must be completed and submitted to the IG team for initial assessment. Contact Information Governance for a copy – **infogov@lhch.nhs.uk**.

## *Information Security Incidents*

Information security incidents are adverse events or near misses that affect or threaten to affect the information or data held by the Trust. Incidents can happen for a number of reasons including but are not limited to:

- Loss or theft of data or equipment storing data e.g. laptops, data sticks
- Inappropriate access of records and unauthorised use data
- Loss or theft of confidential documents e.g. lost diaries, missing case notes
- Misdirected emails or fax messages
- Equipment failure
- Sharing passwords
- Human error e.g. incorrectly addressed mail

Any incident involving personal information has the potential to be classified as an information governance serious untoward incident because what may seem to be of minor importance initially can after further investigation turn out to be much more significant.

## Definition of an information governance serious untoward incident (SUI)

'Any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals should be considered as serious'.

This definition applies irrespective of the media involved and includes both loss of electronic media & data and paper records.

The potential harm to the individual data subject is the overriding consideration when dealing with information security incidents and data breaches. The harm that can occur includes exposure to identity theft through the release of non-public identifiers e.g. passport number and information about the private aspects of a person's life becoming known to others e.g. financial circumstances / medical history.

The extent of harm is dependent on both the volume of personal data involved and the sensitivity of the data.

### How to report information security incidents

All incidents must be reported in line with the Trust's Incident Reporting policy and procedure. If you witness or are made aware of an incident or near miss affecting the security of data complete the Trust's Incident Report Form or report online using the **online Incident Reporting** system. Please include the following:

- Date, time and location of the incident
- Description of what happened:
    - Theft, accidental loss, inappropriate disclosure, procedural failure; lost in transit etc.
    - The number of records / individuals involved
    - If electronic, whether the data had been encrypted or not
    - The type and sensitivity of record / data involved e.g. name, address, medical condition
- Immediate action taken
- Contact details of incident reporter and line manager

The Information Governance team will investigate and categorise incidents, managing SUIs in line with Department of Health guidelines (Gateway Ref: 13177).

Further guidance can be found in the **Information Security Incident Reporting and Awareness leaflet** , Trust **Information Governance policies** and the **ISMS policy and procedures**.

## Training and awareness

All NHS employees are required to complete Information Governance training annually; this includes all part time, full time and temporary members of staff who are employed with the Trust for a period of 3 months or more. Information Governance training can be found in the Trust's mandatory training workbooks

## Glossary of Terms

**Anonymised information:** Information which does not identify an individual directly and which cannot reasonably be used to determine identity. Anonymisation requires the removal of name, address, full post code and any other detail or combination of details that may lead to identification.

**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

**Confidential data or information:** see 'Personal confidential data'

**Consent:** The approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should no 'no surprises') and they should understand the implication of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent.

**Data controller:** Means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

**Data processor:** Means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

**Data subject:** Means an individual who is the subject of personal data.

**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.

**Explicit consent:** This means articulated patient agreement. The terms are interchangeable and relate to a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear.

**Implied consent**: Is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed.

**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.

**Identifiable information**: see 'Personal confidential data'

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

- Name, address, full post code, date of birth;
- Pictures, photographs, videos, audio-tapes or other images of individuals;
- NHS number and local patient identifiable codes;
- Anything else that may be used to identify an individual directly or indirectly.

**Implied consent:** Is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed.

**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.

**Information sharing protocols or agreements:** Documented rules and procedures for the disclosure and use of patient information, which specifically relate to security, confidentiality and data destruction, between two or more organisations or agencies

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

**Medical purpose:** As defined in the Data Protection Act 1998, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001 explicitly broadened the definition to include social care

**Personal confidential data:** This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this guide 'personal' includes the Data Protection Act (DPA) definition of personal data, but it is adapted to include dead as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the DPA. Used interchangeably with 'confidential' in this document.

**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.

**Pseudonymised information (de-identified):** Similar to anonymised information or data in that it cannot reasonably be used to identify an individual however it differs in that the original provider may retain a means of identifying individuals. This is often achieved by attaching codes or other unique references to information so that the data will only be identifiable to those with access to the key or index. Pseudonymisation allows information about individuals to be linked.

**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.

**Sensitive personal data/information:** Data that identifies a living individual consisting of information as to his or her: racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life, convictions, legal proceedings against the individual or allegations of offences committed by the individual. See also 'Personal confidential data'

Handbook compiled with thanks to NHS Central Lancashire and Bridgewater Community Healthcare NHS Trust