**DATA PROTECTION.**

This Act provides the main legislative framework for confidentiality and information sharing issues. The Act stipulates eight principles that must be followed when personal information is "processed" by organisations. (**"Processing"** refers to any work done with personal information including obtaining, recording, viewing, listing, disclosing and destroying.) The Act stipulates the conditions under which information may be shared i.e. the legal justifications.

**The eight principles of the Data Protection Act:**

**1.Fair and lawful**: Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless certain conditions are met, also the processing must adhere to the *fair processing code.*

**2. Use for specified purposes**:

Personal data shall be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

**3. Adequate, relevant and not excessive**: Personal data shall be adequate, relevant and not excessive in relation to the purpose.

**4. Accurate and up to date**: Personal data shall be accurate and, where necessary, kept up to date.

**5. Don't keep longer than necessary**: Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

**6. Rights given under the act**: Personal data shall be processed in accordance with the rights of the data subject under this act".

**7. Security**: Appropriate and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

**8. Disclosure outside Europe**: Personal data shall not be transferred to a country outside the European Economic area, without adequate protection.

**The Caldicott Committee** produced their report on the "Review of Patient Identifiable Information" in December 1997. Caldicott guidance applies to all NHS organisations and local authority Social Services Departments. Guidance is based on six key principles. Organisations are required to appoint Caldicott Guardians to oversee the confidentiality / information sharing process.

**The Code of Practice** was issued in July 2003 and applies to all NHS organisations. It is a guide to required practice on confidentiality, security and disclosure of personal information.

**The six Caldicott Principles:**

**1. Define Purposes**: Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

**2. Use anonymised information if possible**: Patient-identifiable information items should not be included unless it is essential for the specified purpose. The need for patients to be identified should be considered at each stage of satisfying the purpose.

**3. Use the minimum information necessary**: The minimum amount of identifiable information should be transferred or made accessible that is necessary for a given function to be carried out.

**4. Access to personal information on a need to know basis**: Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that

they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

**5. Staff must be aware of their responsibilities**: Action should be taken to ensure that those handling patient-identifiable information – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

**6. Use only when lawful:** Every use of patient-identifiable information must be lawful.

**HUMAN RIGHTS.**

This Act incorporates **Article** 8 of the European Convention of Human Rights which provides that everyone has the right to respect for their private and family life, home and correspondence.

**WHAT INTELLIGENCE SOURCES ARE AVAILABLE TO YOU?**

This information may be received from a variety of sources including:

**The pharmacist dispensing the prescription** e.g. concern raised by an individual prescription or by a pattern of prescribing originating from an individual general practitioner or practice;

**The doctor's partners or nursing colleagues** e.g. concerns about a practitioner prescribing outside of local guidelines or reporting concerns about the practitioner himself;

**Local drugs misuse services** e.g. concerns about a practitioner prescribing outside of local guidelines or not cooperating with shared care guidelines;

**Another general practice** concerns about the prescribing at a patient's previous practice;

**The Prescription Pricing Division of NHS Business Services (PPD)** e.g. if the cost and volume of prescribing triggers preset alarm systems;

**Local audits and monitoring** e.g. preset ePact audits of CDs; the template audit tool on the NPC web-site or locally developed systems;

**The patient or someone acting on their behalf;**

**Excessive stock ordering by a practice or practitioner;**

**Local police information** e.g. an increase in street availability;

**Other sources from within the PCT prescribing team** e.g. practice pharmacists or locums

**How do you disseminate your intelligence? What intelligence system do you have?**

If there are concerns regarding the source of the information or a risk to others is identified through evaluation of the content, a further risk assessment will take place when the report is evaluated for dissemination and the handling codes are applied. These should be agreed at a top level in the Organisation - preferably with the help of your CDLO.

The risk assessment process also includes consideration of ethical, personal and operational risks in respect of the source, the information content, its use, dissemination and compliance with a legislative requirements.

This process will also include a justification for the decisions made and appropriate authority.

It will consider the proportionality, accountability and necessity for recording, disseminating and retaining the information.

## What makes an effective LIN ?

**PEOPLE.**

With appropriate skills and knowledge and up to date training.

**SOURCES OF INFORMATION**

Internal and external:

**KNOWLEDGE.**

Best practice, Current legislation and case law and Training.

**SYSTEMS.**

Collection, reception, recording, storage and use of Information:

Effective briefing and debriefing.

Information exchange protocols.

The AO must maintain a high degree of knowledge and expertise and be supported by everyone in the organisation and ensure that they understand the AO function and contribute to it.

**List types of evidence and give an example.**

**Real evidence** is a type of physical evidence and consists of objects that were involved in a case or actually played a part in the incident or transaction in question. **Direct evidence** supports the truth of an assertion (in criminal law, an assertion of guilt or of innocence) directly, i.e., without an intervening inference. Circumstantial evidence, by contrast, directly supports the truth of evidence, from which the truth of the assertion may be inferred.

For example: a witness who testifies that he saw the defendant shoot the victim gives direct evidence. A forensics expert who says that ballistics proves that the defendant's gun shot the bullet that killed the victim gives circumstantial evidence, from which B's guilt may be inferred.

In direct evidence a witness relates what he or she directly experienced. (Usually the experience is by sight or hearing, though it may come though any sense, including touch or pain.

An **expert witness**, **professional witness** or **judicial expert** is a witness, who by virtue of education, training, skill, or experience, is believed to have expertise and specialised knowledge in a particular subject beyond that of the average person, sufficient that others may officially and legally rely upon the witness's specialized (scientific, technical or other) opinion about an evidence or fact issue within the scope of his expertise.

**Documentary evidence** is any evidence introduced at a trial in the form of documents. Although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually include any media by which information can be preserved. Photographs, tape

**Circumstantial evidence** is evidence in which an inference is required to connect it to a conclusion of fact. By contrast, direct evidence supports the truth of an assertion directly—i.e., without need for any additional evidence or the intervening inference. On its own, it is the nature of circumstantial evidence for more than one explanation to still be possible. Inference from one piece of circumstantial evidence may not guarantee accuracy. Circumstantial evidence usually accumulates into a collection, so that the pieces then become corroborating evidence. Together, they may more strongly support one particular inference over another. An explanation involving circumstantial evidence becomes more valid as proof of a fact when the alternative explanations have been ruled out.

**Hearsay** is information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience. When submitted as evidence, such statements are called **hearsay evidence**. As a legal term, "hearsay" can also have the narrower meaning of the use of such information as evidence to prove the truth of what is asserted. Such use of "hearsay evidence" in court is generally not allowed. This prohibition is called the **hearsay rule**.

For example, a witness says "Susan told me Tom was in town". Since the witness did not see Tom in town, the statement would be hearsay evidence to the *fact* that Tom was in town, and not

admissible. However, it *would* be admissible as evidence that Susan *said* Tom was in town, and on the issue of her knowledge of whether he was in town.

In England and Wales, hearsay is generally admissible in civil proceedings[4] but is only admissible in criminal proceedings if it falls within a statutory or a preserved common law exception, all of the parties to the proceedings agree, or the court is satisfied that it is in the interests of justice that the evidence is admissible.

**HSWA 1974:**

**37. Offences by bodies corporate.**

— (1) Where an offence under any of the relevant statutory provisions committed by a body corporate is proved to have been committed with the consent or connivance of, or to have been attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate or a person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, the preceding subsection shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

**36. Offences due to fault of other person.**

— (1) Where the commission by any person of an offence under any of the relevant statutory provisions is due to the act or default of some other person, that other person shall be guilty of the offence, and a person may be charged with and convicted of the offence by virtue of this subsection whether or not proceedings are taken against the first-mentioned person.

(2) Where there would be or have been the commission of an offence under section 33 by the Crown but for the circumstance that that section does not bind the Crown, and that fact is due to the act or default of a person other than the Crown, that person shall be guilty of the offence which, but for that circumstance, the Crown would be committing or would have committed, and may be charged with and convicted of that offence accordingly.

## Corporate Homicide and Corporate Manslaughter Act 200

The Corporate Manslaughter and Corporate Homicide Act 2007 introduced across the UK a statutory offence of 'corporate manslaughter'. This page provides information about the Act and its implementation.

Introduction to the Act

The Act introduced a new statutory offence of corporate manslaughter, allowing for the prosecution of a wide range of organisations across the public and private sectors where gross

failures in the management of health and safety resulted in the death of a person to whom the organisation owed a duty of care.

Most of the Act came into force on 6 April 2008, while the implementation of the 'custody provisions' contained in Section 2(1)(d), which make the Act applicable to the management of custody came into force on 1 September 2011.

***Briefly, the Corporate Manslaughter Act:***

- Makes it easier to prosecute companies when gross failures in the management of health and safety led to a death by removing the previous common law requirement that a 'directing mind' (such as a director) at the top of the company should also be personally liable.
- Applies to companies and other corporate bodies, in the public and private sector, government departments, police forces and certain unincorporated bodies, such as partnerships, where these are employers.
- Does not create any new duties or require organisations or businesses to comply with new regulatory standards.
- Is concerned with the corporate liability of the organisation itself, not with the individual liability of directors, senior managers or other individuals. However, where there is sufficient evidence of individual liability, individuals can also be prosecuted for gross negligence manslaughter and for health and safety offences. The Act does not change this position.

## Guidance on the Act

The link below provides a general introduction to the Act for employers, senior managers and others seeking an overview of the new legislation, explaining how the offence of corporate manslaughter works and where it will apply.

Understanding the Corporate Manslaughter and Corporate Homicide Act 2007

The following documents provide further detail on the Act, and are intended for those who need to understand how the Act works, including health and safety managers and criminal justice professionals.

Corporate Homicide and Manslaughter Act 2007

Guide to the Corporate Manslaughter and Corporate Homicide Act 2007

The following are useful web links which will give you further information on the relevant legislation and guidance.

Further help regarding the LIN can be found across the web by typing in Local Intelligence Network. You will see various documents published by many Authorities across the UK.

**HSWA 1974**

*www.hse.gov.uk/**legislation**/hswa.htm*

**The Data Protection Act 1998**

*www.legislation.org.uk/*

**Caldicott principles - Health Protection Agency**

*www.hpa.org.uk*

**Human Rights Act 1998 - The Articles**

http://www.legislation.gov.uk/ukpga/1998/42/schedule/1

**Corporate Homicide and Corporate Manslaughter Act 2007**

http://www.justice.gov.uk/legislation/bills-and-acts/acts/corp-hom-manslaughter-act-2007