GUIDANCE ON HOW CALDICOTT PRINCIPLES RELATE TO TRUST INFORMATION POLICY AND PROCEDURE

OBJECTIVE:
To provide additional guidelines to staff and service users to support the Trust's commitment to information security and confidentiality

What is 'Caldicott'?
A review was carried out in 1997 by the Caldicott Committee to investigate ways in which service user information is used within the National Health Service. The aim was to improve the quality of, and protect service user information. The investigation identified certain principles that NHS organisations should adopt, these are known as the Caldicott Principles.

As part of the recommendations each National Health Service body was tasked with identifying a senior director to take responsibility and act as the 'Caldicott Guardian'.

Who is the Caldicott Guardian?
Lancashire Care Trust's Caldicott Guardian is currently Professor Max Marshall, Executive Medical Director who is based at the Trust Headquarters, Sceptre Point, Walton Summit, Preston, PR5 6AW.

What does he do?
The Caldicott Guardian ensures that high standards of patient and personal information security and confidentiality are implemented throughout the Trust. The Caldicott Guardian ensures that confidentiality is a trust priority and relevant issues are represented at Board level.

There are six 'Caldicott' principles that also tie in with the seven principles of the Data Protection Act 1998.

Principle One
Justify the purpose(s) of using confidential information
The use or transfer of patient-identifiable information within or from an organisation should be clearly defined and regularly reviewed
The Trust completes an annual submission of patient identifiable data held to the Information Commissioner. The Trust holds information under six categories, these are:

- Staff Administration including volunteers, agents, temporary and casual workers
- Accounts & Records
- Health Administration and Services, i.e. provision and administration of patient care.
- Research in any field, including market, health, lifestyle, scientific or technical research.
- Crime Prevention and Prosecution of Offenders
- Public Health, the prevention and control of disease within the Community

Principle Two
Only use it when absolutely necessary
Patient-identifiable information items should not be included unless it is essential.
Staff must obtain awareness of the systems and processes currently in place that ensure personal information is not inappropriately disclosed, for example adopting safe procedures for answering telephone queries, the use of fax machines and information sharing protocols that set out the terms on which personal information may be shared with an external organisation.
Guidance must also be observed on the avoidance of inadvertent disclosure caused by discussion of patient details in inappropriate venues, e.g. the canteen, in the lift, on the bus, etc.
When exchanging information, particularly with other organisations through electronic communications, information should normally be be "anonymised". For example, rather than using a person's full name and other information that could easily identify them, using their NHS number is good practice.
By taking personal information out of communications (wherever possible) we reduce the risk of breaches of confidentiality.
Confidential information, especially patient information, should never be sent via email to any Internet based e-mail address. The Internet is not considered a secure "zone".
Anyone who is not sure about the safety of the recipient's e-mail should always take advice from the IT department before sending such a message.

Principle Three
Use the minimum that is required
Only the minimum amount of identifiable information should be transferred or accessible as is necessary for a given function.
Staff should be made aware that even where there is a genuine reason to disclose personal information this will not often require the whole of a patient's record to be disclosed.

In order to reduce the risk of data loss or breaches of confidentiality, try not to use excessive amounts of information. Don't make a patient's entire case history available to someone who only needs a particular snippet of information from it.

Principle Four
Access should be on a strict need-to-know basis
Only those individuals who need access to patient-identifiable information should have access to it, limited to what they need to see.
Always take care not to let sensitive information fall into the wrong hands. People, who ask for information such as solicitors, other NHS organisations, or even the Police, aren't always legally entitled to request it.
It's also worth taking extra care when saving information on a computer system. Putting computer files into incorrect places on the system may mean that unauthorised people may be able to access sensitive information. When using electronic clinical care records it is essential that passwords are not shared and that staff log out of the system if they leave their computer unattended.

Principle Five
Everyone must understand his/her responsibilities
Action should be taken to ensure all staff are made fully aware of their responsibilities and obligations to respect patient confidentiality
Simply being aware of the fundamental need for confidentiality, integrity and availability of information will help you make the right decisions.

Ensure that you are familiar with the Trust's acceptable use policies. There are specific clauses in your employment contract relating to confidentiality.
Also be sure to familiarise yourself with the content of the Trust's IT User Code of Practice. This is available on the Information Governance intranet site.

Principle six
Understand and comply with the law
Every use of patient-identifiable information must be lawful.
Thankfully not everyone is expected to be an expert in information law. Most of the time it's likely that the information you work with will be within established procedures or within the defined scope of information systems.
However from time to time you may find that a particular task means you have to use or exchange information in a way that you haven't done before, that may not fit anywhere within established procedures.
In such a situation it is always best to check with secondary guidance via your line manager if in doubt around any legal implications or other information security risk.

Trust Contacts:
Professor Max Marshall
Caldicott Guardian
Max.marshall@lancashirecare.nhs.uk

Dr John McKenna
Deputy Caldicott Guardian
John.mckenna@lancashirecare.nhs.uk

Dave Tomlinson
Senior Information Risk Owner / Executive Director of Finance
Dave.tomlinson@lancashirecare.nhs.uk

Peter Holden
Health Records Advisor
Peter.Holden@lancashirecare.nhs.uk

Michelle J Brammah
Information Governance Lead
michelle.brammah@lancashirecare.nhs.uk

Sue Stone
Information Governance Specialist
Sue.stone@lancashirecare.nhs.uk

Related LCFT Guidance/Procedures

The Trust has a range of policies and procedures to support compliance with Caldicott principles. These can be accessed in the Freedom of Information Publication Scheme

http://www.lancashirecare.nhs.uk/contact-us/FOI-Information/FOI-Publication.php