Legislation

Data Protection Act 1998 (8 Principles)

There are 8 Data Protection principles which regulate the use of person identifiable data (personal data). Any use of personal data should be:

1. Fair and lawful
2. Used only for specified and lawful purposes
3. Adequate, relevant and not excessive to need
4. Accurate and kept up to date
5. Not kept for longer than necessary
6. Processed in accordance with data subject rights, including rights of access.
7. Kept secure and protected against accidental disclosure, loss or damage
8. Not transferred outside the EEA

Human Rights Act 1998

Article 8: Everyone has the right to respect for his private and family life, home and correspondence.

It is unlawful for a public authority to act in a way that is incompatible with a Convention right.

Common Law Duty of Confidence

Information obtained for one purpose should not be used for another purpose without the express or implied authorisation (consent) of the provider of that information.

Further Information

Caldicott Guardian

Dr Andrew Dove Ext: 61764

Caldicott & Data Protection Adviser

Debbie Terry Ext: 47169

Information Security Adviser

David Cadwell Ext 47100

ICT Services Helpdesk

City Hospital Campus Ext 47777
QMC Campus Ext 69000

Trust policies and guidance are available on the Trust's Intranet site:

http://nuhweb/

The latest Information Security policies, confidentiality guidance and leaflets are available for download from the Trust's Information Security Intranet site:

http://intranet/infosec/

See also the "General Protocol for Information Sharing Between Health and Social Care Agencies in Nottingham" issued in 2006.

Nottingham University Hospitals NHS
NHS Trust

Security and Confidentiality of Patient and Personal Information




Issued on behalf of the Nottingham Caldicott Guardian Forum

Introduction

All employees of the Trust are responsible for maintaining confidentiality. This duty of confidentiality is written into employment contracts. Breach of confidentiality of information gained, either directly or indirectly in the course of duty is a disciplinary offence that could result in dismissal.

Staff are authorised to have access to patient information they need to know in order for them to perform their duties. Gaining access or attempting to gain access information that you do not need to see to carry out your work is a breach of confidentiality as is passing information on to someone who is not authorised to receive it.

Any personal information, non-clinical or clinical, must be treated as confidential.

The general principles underlying the use and sharing of personal information follow the Caldicott Principles:

- Justify the purpose for using patient confidential information.
- Only use patient identifiable information when absolutely necessary.
- Use the minimum identifiable information required for that purpose.
- Access should be on a strict need-to-know basis only.
- Everyone must understand their responsibilities to protect information, and
- Everyone must understand and comply with the law.

Basic Principles

Any personal information given for one purpose must not be used for another purpose without the consent of the individual concerned because that use may breach confidentiality.

A patient's right to confidentiality is protected by ethics and the law.

Patients have a legal right to know what information is being collected and why, and the purposes for sharing that information.

In some circumstances they have a right to choose how their personal data may be used or who is allowed to see it.

Every member of staff has an obligation to protect confidentiality and a duty to verify the authorisation of another person to ensure information is only passed on to those who have a right to see it.

The rules are there to protect both the patient and staff from breaches of confidentiality, but they should not be applied so rigidly that they are impractical to follow or detrimental to the care of the individual concerned.

All staff should understand their responsibility to protect the confidential information they collect and use, by following the rules and guidance that are available to them.

You are Responsible for Your Decision to Pass on Information

If you are unsure about whether or not to disclose information, consult your Line Manager and/or, if necessary, obtain advice from your organisation's Caldicott Guardian, Caldicott & Data Protection Adviser or Information Security Adviser.

Duty of Care

All reasonable care should be taken to protect the physical security of confidential information from accidental loss, damage, destruction, unauthorised access or accidental disclosure.

For example:

- Do not use someone else's password to gain access to information held on the computers.
- Confidential data held on computers, laptops or disk should be kept physically secure and password protected.
- Confidential patient information should not be sent via the Internet without being adequate protection against unauthorised or accidental disclosure.
- Patient information should be kept secure and not left unattended and available for the patient or public to see.
- Faxing is not secure. Confidential information should be faxed only when there is no alternative and immediate receipt is absolutely necessary for clinical purposes. 'Safe Haven'[1] procedures should be followed.
- Envelopes containing patient/client confidential information must be securely sealed, labelled 'Confidential' and clearly addressed to a known contact.
- Telephone 'validation procedures'[2] must be followed to confirm the identity of telephone callers before information is given to them.
- Follow the Trust's Information Security and Data Protection policies and procedures and seek advice when in doubt.

1 Safe Haven (EL (92(60) – an agreed set of administrative and physical security procedures for minimising the risk of breach of confidentiality when sending information via fax – See Trust policy for further information.

2 The details of the callers published telephone number (not direct dial or mobile phone numbers) should be obtained checked against a known directory and a telephone call made back to ensure authenticity – See Trust validation Guidance.